CLOUDFLARE

WHITEPAPER

CAF Compliance with Connectivity Cloud

Achieving compliance with Secure Access Service Edge (SASE)

Content

Preparing for CAF compliance with Connectivity Cloud

The National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) details key cybersecurity principles to guide all organisations that provide critical services or hold sensitive information. The CAF Collection has four top-level objectives that, if achieved, will help protect the UK's economy, society, environment, and general welfare. They include:

- Objective A: Managing security risk
- Objective B: Protecting against cyber security attack
- Objective C: Detecting cyber security events
- Objective D: Minimising the impact of cyber security incidents

Each objective includes a set of specific principles meant to help organisations enhance their cyber resilience, many of which require modern technology to accomplish.

This whitepaper describes how Cloudflare's Secure Access Service Edge (SASE) can help public sector organisations achieve and demonstrate compliance with the CAF Collection. SASE delivers several network security functions via a cloud-native service that inspects and protects traffic flowing through an organisation's wide area network (WAN).

Eight SASE capabilities essential for CAF compliance include:

1. Data encryption and protection
2. Access management
3. Operational resiliency
4. Data minimisation and privacy
5. Security integration
6. Malware detection and prevention
7. Incident detection and response
8. Logging and monitoring

Data Encryption and Protection

Defending against unauthorized access and disclosure

Public sector organisations are entrusted with highly sensitive information. Therefore, the Data Security principle (under Objective B) guides organisations to secure this data with well-tested cryptographic suites, both in-transit and at-rest.

SASE connects geographically distributed sites with secure, virtual private links. All traffic flowing over the SASE network is encrypted, protecting against potential eavesdropping and unauthorized access to sensitive information. It combines the power of Zero Trust Network Access (ZTNA), Software-Defined WAN (SD-WAN) and Smart Routing to optimally route traffic over available transport media. This both enhances traffic performance and improves network resiliency by allowing seamless recovery from link outages.

The Data Security principle is more than just bolting on encryption, though. "Design to protect data" means that networks and information systems have data protection built into their fundamental architecture. Cloudflare's global backbone uses a device-light, cloud-heavy approach designed for unparalleled data security. Here's how:

- **Automated threat detection:** The first of these is the detection of potential threats to the sensitive data in an organisation's care. For example, Cloudflare offers multi-channel protection against phishing attacks. These defenses can identify and block attempts to steal user credentials or sensitive data via email, corporate messaging apps, and other platforms.
- **Data loss prevention (DLP):** SASE solutions also integrate DLP capabilities to identify suspicious outbound data flows. DLP can be configured to identify common types of sensitive data, such as payment card data or government identification numbers.
- **Advanced analytics:** It also employs machine learning and behavioral analytics to detect and block unusual data flows.

Access Management

Controlling access to data and services

SASE offers integrated Zero Trust security for the corporate WAN.

Zero Trust is the next generation of identity and access management (IdAM). Under a Zero Trust security model, users and devices are granted access to resources on a case-by-case basis. These access decisions are based on least privilege access controls and assessments of the risk associated with a request.

Zero Trust Network Access (ZTNA) capabilities are a core component of SASE, managing access to the corporate network and connected resources. ZTNA replaces traditional virtual private networks (VPNs), which provide authenticated users with unrestricted access to the corporate network and have themselves become a security risk and active security target due to legacy code bases and the ease of disruption with DDoS attacks.

CAF Principle B2 Identity and Access Management (IdAM) specifies how organisations should control access to their networks and devices. Cloudflare's SASE toolset Cloudflare One offers key IdAM capabilities, including:

- **Application-Specific Access Management:** Cloudflare One uses software-defined networking (SDN) and an understanding of various types of application traffic to apply granular access controls to requests for organisational resources. All traffic enters and leaves the corporate WAN, SaaS toolsets and Cloud Resources via a SASE endpoint, whether a remote user or network level firewall. This ensures that all traffic is inspected, and unauthorized requests are blocked before they reach their intended destination.
- **User and Device Authentication:** SASE's integrated ZTNA capabilities enable public sector organisations to effectively implement role-based access control (RBAC) at scale. This also includes authenticating devices used to access organisational resources and performing the monitoring and management of privileged users required by CAF.
- **Network Monitoring and Troubleshooting:** ZTNA's granular control over access requests also provides organisations with valuable visibility into network utilization. This not only enhances security monitoring but can be useful for troubleshooting and infrastructure optimization.
- **SaaS Access and Configuration Management:** Cloud access security broker (CASB) and cloud security posture management (CSPM) solutions also enable robust access management for cloud environments by enforcing corporate policies, managing access, highlighting risks, performing data classification, detecting shadow IT usage and providing controls points for Software as a Service (SaaS) apps.

Operational Resiliency

Ensuring availability of data and services

Cloud-based SASE solutions can greatly enhance network resiliency and protection against cyber threats

UK public sector organisations are responsible for ensuring that public data and services are accessible to citizens and UK businesses. At the same time, government organisations are a prime target for hacktivists and other cyber threat actors.

The Cloudflare network enhances resiliency via redundant, geographically-distributed systems, in-line with CAF Principle B5 Resilient Networks and Systems. These include:

- **Intelligent Network Routing:** Once traffic enters the Cloudflare network, it is directed over an optimized route identified via ML-learning based smart routing. This offers a low-latency, predictable, and reliable connection to its exit point from the Cloudflare network.
- **Distributed Infrastructure:** SASE's decentralized nature also provides built-in redundancy for the corporate WAN. Cloudflare operates six data centres in the UK and hundreds worldwide. Even severe events, such as natural disasters, have minimal impacts on performance and uptime as each data centre provides identical SASE capabilities, and critical data is cached at multiple sites.

Maintaining availability also requires resiliency in the face of distributed denial-of-service (DDoS) attacks and similar threats. With the scale of modern attacks, highly redundant infrastructure may not be enough as cybercriminals can still overwhelm it.

CAF Requirement B5.b Design for Resilience mandates that networks and information systems supporting essential functions be resilient to cybersecurity incidents. In addition to core SASE functions, the Cloudflare network offers the following capabilities to address these requirements:

- **DDoS Mitigation:** DDoS attack traffic is identified and filtered as it enters the Cloudflare network, preventing it from reaching target systems and affecting the experience of legitimate users.

- **Content Distribution Networks (CDNs):** CDNs enhance operational resiliency by reducing dependence on the headquarters network and origin servers. CDN locations are globally distributed and can serve cached content even if the origin server is unavailable.

Data Minimisation and Privacy

Reducing the risk of data leaks or misuse

Limiting data storage and processing reduces the risk of data misuse or leaks.

Public sector organisations are commonly targeted by advanced persistent threats (APTs) with the resources of nation-states or organized crime supporting them. Data minimisation reduces an organisation's exposure to these threats since it can't leak data that it doesn't have. Similarly, data minimisation can enhance user privacy by ensuring that data isn't stored or processed without appropriate consent and authorisation.

As specified in CAF Requirement B3.a, Understanding Data, data visibility is critical to data security. SASE's ZTNA and DLP capabilities offer insight into data flows within the organisation by monitoring access requests for corporate resources and flows of sensitive data outside of the organisation's network.

Cloudflare's security solutions are also designed to offer robust threat detection while minimising access to sensitive data and ensuring user privacy. With access to threat intelligence and security data on a global scale, Cloudflare can identify non-obtrusive indicators of compromise (IoCs) to detect potential threats.

For example, a phishing email may be identified by using natural language processing (NLP) to analyze the email's contents for common phishing techniques. However, if the sender's IP or email address is known to be associated with a cybercrime group, this level of in-depth analysis is unnecessary.

Security Integration

Streamlining security and eliminating blind spots

Integrating security and network functions improves efficiency and reduces the risk of security gaps.

SASE was invented to address one of the major challenges faced by organisations around the world: security complexity. Companies that deployed various security tools to address specific risks or environments created complex security architectures that were difficult to monitor, manage, and configure correctly. This resulted in major security and visibility gaps, overwhelmed security teams, and undermined confidence in their security infrastructure.

Cloudflare One streamlines risk management and enhances security assurance via:

- **Converged Security:** SASE solutions integrate various key network security functions, including NGFW, IDS, WAF, and more into a single, cloud-native solution. This security integration simplifies implementation, reduces network latency, and decreases the risk of security gaps.
- **Integrated Intelligent Routing:** SASE also incorporates SD-WAN functionality for optimized network routing. This not only improves network efficiency and performance but also ensures that all traffic passes through a SASE endpoint for inspection. As a result, organisations benefit from improved security and increased visibility into the traffic traversing their networks.

This integration of security and network infrastructure exemplifies the principle of security by design (CAF B4.b). If security is built into the system from the start, it is often more efficient and effective than if it were "bolted on" afterward.

The integrated network visibility that SASE provides is also essential for organisational risk management and strategic planning. Single-pane-of-glass network visibility and management provides a clear view into the risks that the organisation faces and the effectiveness of the security solutions for managing these risks.

Malware Detection and Prevention

Reducing malware risks through proactive security

Ransomware and other malware have emerged as a leading threat to organisations' data security and service availability.

Malware attacks have grown more sophisticated and widespread in recent years, due to the growth of the cybercrime economy and the recent introduction of generative AI (GenAI). Relationships between cybercrime groups provide increased access to advanced malware, and GenAI can automatically write advanced malware with evasive capabilities.

Key elements of Cloudflare One's defence-in-depth strategy to address the malware threat include:

- **Inbound Malware Detection:** SASE includes various functions for inbound malware prevention, such as NGFWs, IDS/IPS, and RBI. For example, remote browser isolation (RBI) prevents malware from being downloaded from webpages by running web browsers in a sandboxed environment where malicious code can't infect a user's computer.
- **IP and Domain Filtering:** Malware can also be identified based on its attempts to establish communications with command and control (C2) infrastructure. Requests to known malicious IP addresses or domains can be blocked and used as potential indicators of compromise (IoCs) for an infected host.
- **Data Loss Prevention (DLP):** As ransomware groups pivot to focus on data theft and extortion rather than encryption, preventing data exfiltration can help to mitigate the potential impacts of a successful intrusion. SASE's integrated DLP functionality can identify and block anomalous data flows or ones carrying sensitive data outside of the organisation.

Incident Detection and Response

Detecting and mitigating potential intrusions

Threat intelligence and comprehensive visibility are essential for rapid responses to security incidents.

CAF Principle D1.b Response and Recovery Capability acknowledges the importance of timely information for effective incident response. The faster an organisation can identify and address a threat, the less impact it has on the business.

Cloudflare One enhances security visibility and control by consolidating visibility and key capabilities into a single solution. The incident detection and response are improved via:

- **Security Integration:** Integrated security solutions can take advantage of additional context to more accurately identify potential attacks. Displaying security data in a single dashboard eliminates time-consuming context switching and reduces the risk that vital data will be overlooked.
- **Threat Intelligence:** A robust incident detection and response program starts with high-quality threat intelligence. By automatically ingesting threat intelligence, SASE solutions ensure that their various security functions have the data required to identify the latest threats and attack campaigns.
- **Consolidated Dashboards:** Consolidating security monitoring and management into a single dashboard simplifies alert triage and security monitoring. A single source of high-quality alerts reduces time wasted on false positives and streamlines SOC processes.
- **Centralized, Automated Remediation:** If security teams identify a threat, Cloudflare One empowers them to rapidly take action to remediate it across the entire corporate WAN. From a single console, security teams can push out updated firewall rules, lock down compromised accounts, and perform additional analysis to identify the root cause and potential effects of the suspected intrusion.

Logging and Monitoring

Maintaining visibility and identifying issues

Security logs support incident response, digital forensics, and regulatory compliance.

CAF Principle C1 Security Monitoring underscores the importance of data for an effective security program. While alerts draw attention to security incidents, logs are critical to achieving the required context to understand what has occurred and to support threat hunting or compliance actions.

Cloudflare One simplifies logging and monitoring via:

- **Solution Integration:** With various security functions integrated into a single solution, their logging and monitoring capabilities are combined as well. Providing data access via a single dashboard helps to eliminate visibility gaps and streamlines operations.
- **Built-In Threat Intelligence:** With access to Cloudflare threat intelligence feeds, SASE maximizes the potential impact of log data. High-quality threat intelligence helps to triage event data, enabling the organisation to differentiate between false positives and negatives.
- **Zero Trust Access Management:** The value of log data to the organisation's security operations can also make it a major target for cyber threat actors. An attacker with access to unsecured log data can use the information that it contains to plan future attacks. Additionally, deleting log events can help an attacker conceal their presence by eliminating traces of failed authentication attempts and other potential indicators of compromise (IoCs). ZTNA can help organisations to ensure that log data is properly secured against potential compromise. Implementing least privilege access controls can restrict access to sensitive log data on a need-to-know basis.

Case Study: UK council secures access to government services with Cloudflare Zero Trust

A UK council, responsible for one of England's largest metropolitan boroughs, provides hundreds of services to over 327,000 residents, took steps to modernize its IT infrastructure and improve its defenses against ransomware and other common cyber threats.

After an in-depth search process, the council elected to partner with Cloudflare along with its long-time service provider Agilisys. A key deciding factor was the Cloudflare Connectivity Cloud. Integrating various networking and security capabilities into a single solution simplified management for the busy council.

The council's first priority was implementing a Zero Trust architecture to support its many remote workers. By rolling out Cloudflare Zero Trust Network Access (ZTNA), they ensured that employees and trusted third parties could work from anywhere without compromising security. Zero Trust also helped to ensure that residents' personally identifiable information (PII) was properly protected even when accessed by external partners.

Integrated security features also helped to protect the council's infrastructure against various cyber threats. For example, remote browser isolation (RBI) and secure web gateway (SWG) capabilities helped to block malicious web content from reaching and infecting users' devices.

Cloud accessibility and security was also key. Cloudflare's various serviceintegrations with Microsoft enabled secure, high-performance access to the council's Azure-based applications.

Key Benefits

- Simplified Zero Trust access rules reduces administrative overhead
- Decreased network latency for 4,600 remote government employees
- Reduced costs by eliminating the need for separate laptops for external partners

> **"Cloudflare is helping deliver a faster, more consumer-type feel to our internal environment — which is also now more secure."**
>
> **CISO, UK Council**

Case Study: UK Government Agency/CDS

UK government agency implements secure remote access with Cloudflare and CDS

A UK government agency is responsible for maintaining and ensuring access to a solution of national importance.

This agency and its service provider, CDS, were searching for a solution to offer secure remote access to their backend system. Their primary considerations were managing access to sensitive functionality and protecting against ongoing bot attacks.

After evaluating available solutions, they selected Cloudflare Access as the best option for their use case. Cloudflare Access offered easier management than their existing firewall-based system and enabled them to implement Zero Trust access policies for granular control over the users and devices able to connect to these systems.

The agency elected to deploy Access with shared seats that can be used by any employee or CDS contractor on an as-needed basis. Users can authenticate through their browser, allowing the agency to enforce their access policies while eliminating the need for users to install any software on their devices.

In addition to improved access management, the agency also benefits from enhanced application performance. Cloudflare Bot Management protects the solution against malicious bots, reducing load on the agency's servers.

The agency also uses Cloudflare Tunnel to optimize its application performance. Tunnel implements secure, direct routing between a data centre and the nearest Cloudflare data centre, concealing the application's location and enabling optimized routing over the Cloudflare network.

Key Benefits

- Simplified Zero Trust access rules reduce administrative overhead.
- Decreased malicious bot traffic improves security and application performance.
- Enhanced application performance due to optimized routing via Cloudflare Tunnel.

> **"Cloudflare Access provided the platform with a secure remote access solution right out of the box. It's very easy for the clients to use, and it takes very little time for CDS to maintain."**

Why Cloudflare?

Public sector organisations are responsible for providing critical services to residents and protecting their personal data. At the same time, they struggle with limited funding and are prime targets for cyberattacks.

Cloudflare helps the UK public sector to improve their security posture and CAF compliance through a unified, manageable solution. The Connectivity Cloud offers capabilities that address most network-level CAF requirements and provide protection based on Cloudflare's cutting-edge technology and global threat intelligence.

Cloudflare is trusted by organisations around the world to protect the security of their networks and data and to safeguard their online experiences.

Learn more about how Cloudflare can help you to simplify and enhance your online security today. Talk to our experts to get started.

	ZTNA	SWG	RBI	CASB	CSPM	Email Security	DLP	Magic WAN	Magic Firewall	DDoS Protection	WAF	API Gateway	Management	Logs	Threat Intel	Trust Center	Workers	Pages	CDN
Objective A	**Managing security risk**																		
A1 Governance																			
A1.a Board Direction																			
A1.b Roles and Responsibilities																			
A1.c Decision-making																			
A2 Risk Management																			
A2.a Risk Management Process					X										X				
A2.b Assurance																X			
A3 Asset Management																			
A3.a Asset Management																			
A4 Supply Chain																			
A4.a Supply Chain																X			
Objective B	**Protecting against cyber attack**																		
B1 Service Protection Policies, Processes and Procedures																			
B1.a Policy, Process and Procedure Development	X		X		X	X	X												
B1.b Policy, Process and Procedure																			
B2 Identity and Access Control																			
B2.a Identity Verification, Authentication and Authorization	X			X															
B2.b Device Management	X																		
B2.c Privileged User Management	X													X					
B2.d Identity and Access Management (IdAM)	X			X										X					
B3 Data Security																			

	ZTNA	SWG	RBI	CASB	CSPM	Email Security	DLP	Magic WAN	Magic Firewall	DDoS Protection	WAF	API Gateway	Management	Logs	Threat Intel	Trust Center	Workers	Pages	CDN
B3.a Understanding Data	X							X											
B3.b Data in Transit	X			X		X	X	X											
B3.c Stored Data																			
B3.d Mobile Data																			
B3.e Media / Equipment Sanitisation																			
B4 System Security																			
B4.a Secure by Design					X			X			X	X			X		X	X	
B4.b Secure Configuration	X			X	X									X					
B4.c Secure Management	X	X	X			X					X	X			X				
B4.d. Vulnerability Management	X		X	X	X				X		X	X		X	X				
B5 Resilient Networks and Systems																			
B5.a Resilience Preparation															X				
B5.b Design for Resilience								X									X	X	X
B5.c Backups								X									X	X	X
B6 Staff Awareness and Training																			
B6.a Cyber Security Culture																			
B6.b Cyber Security Training																			
Objective C	**Detecting cyber security events**																		
C1 Security Monitoring																			
C1.a Monitoring Coverage	X													X	X				
C1.b Securing Logs	X													X					
C1.c Generating Alerts														X	X				
C1.d Identifying Security Incidents									X		X	X			X				

	ZTNA	SWG	RBI	CASB	CSPM	Email Security	DLP	Magic WAN	Magic Firewall	DDoS Protection	WAF	API Gateway	Management	Logs	Threat Intel	Trust Center	Workers	Pages	CDN
C1.e Monitoring Tools and Skills									X		X	X		X	X				
C2 Proactive Security Event Discovery																			
C2.a System Abnormalities for Attack Detection														X	X				
C2.b Proactive Attack Discovery																			
Objective D	**Minimising the impact of cyber security incidents**																		
D1 Response and Recovery Planning																			
D1.a Response Plan															X				
D1.b Response and Recovery Capability								X									X	X	X
D1.c Testing and Exercising																			
Principle D2 Lessons Learned																			
D2.a Incident Root Cause Analysis														X	X				
D2.b Using Incidents to Drive Improvements																			

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-6893.2025JAN09