CLOUDFLARE

WHITE PAPER

Cloudflare for Government

Extensive TIC 3.0 security capabilities, accelerated by Cloudflare's global backbone

Modernize your Trusted Internet Connections (TIC) 3.0 program today

From "descriptive to deployed" with Cloudflare

CISA's TIC 3.0 core guidance is "descriptive, not prescriptive," leaving the interpretation and decision-making entirely up to agency decision-makers. While it's flexible, it can also challenging for agencies to comply with a variety of vendor products.

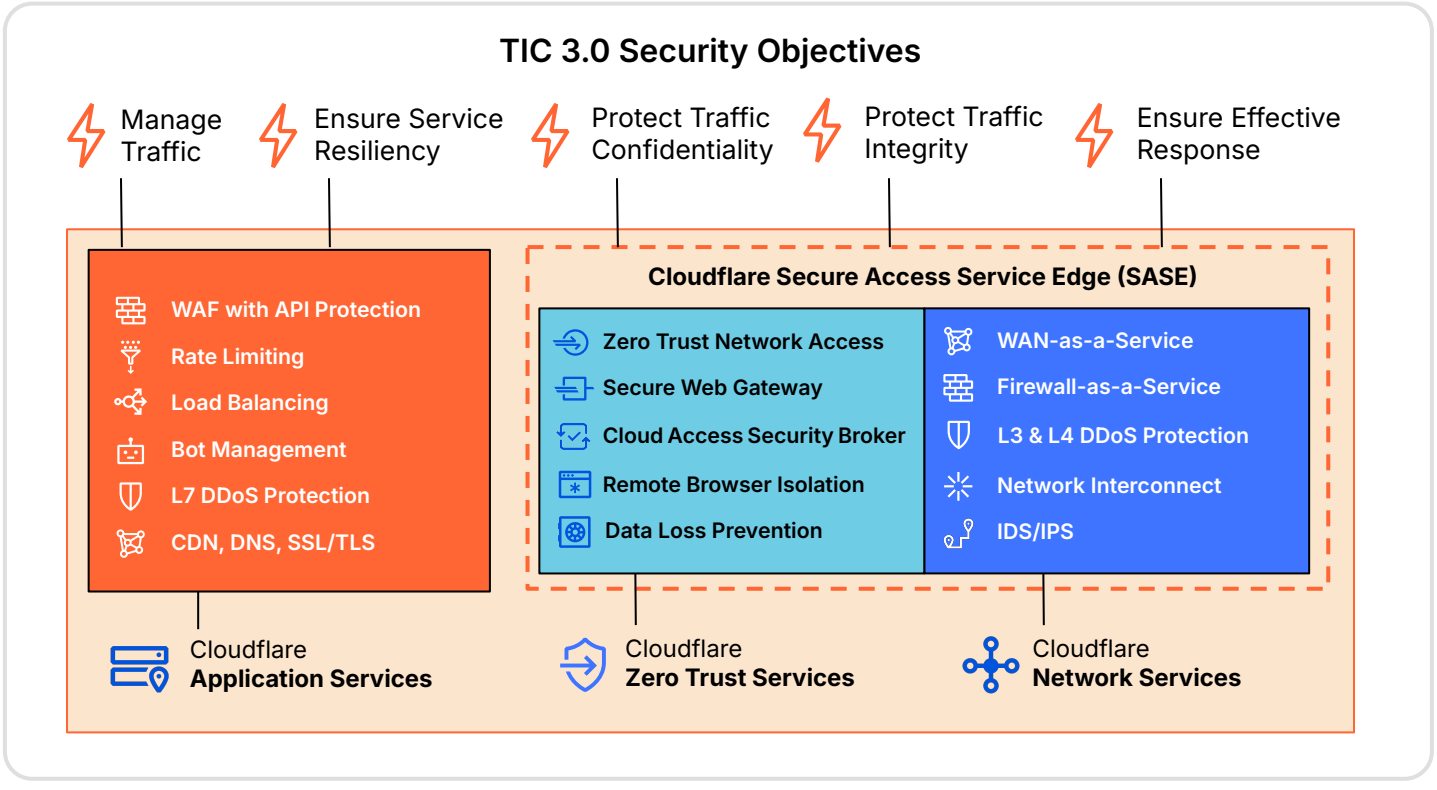
Cloudflare makes it simple. As the Trusted Internet for Government, we deliver modern security capabilities that are essential for both your TIC 3.0 and Zero Trust architectures, all powered by our global network and FedRAMP-authorized solutions.

This paper uses CISA's Overlay Handbook (Volume 5) structure to align Cloudflare's solutions with the Security Capabilities catalog (Volume 3). See for yourself how far our partnership can take you, from modern security to world-class network and application performance to unprecedented efficiency at lightning speed.

Cloudflare for Government

- Every service available now at all 32 FedRAMP data centers.
- No special enclaves that limit the capabilities you need today.
- Direct connections for maximum performance and security.

FedRAMP™



TIC 3.0 Security Capabilities

Security Capabilities are the "descriptive" requirements, found in Volume 3 of CISA's TIC 3.0 Core Guidance. They apply to the TIC Use Cases (Volume 4), which build on the Reference Architecture (Volume 2). There are two main categories of Security Capabilities, Universal (UNI/UNL) and Policy Enforcement Point (PEP), where UNI/UNL capabilities apply to all use cases, while PEP capabilities apply only to certain ones.

Each Security Capability (Volume 3) has a unique identifier that CISA doesn't mention in the Overlay Handbook (Volume 5), but we included those identifiers in this paper to make it easier to cross-reference.

Universal (UNI/UNL) Security Capabilities

Enterprise-level security capabilities that outline guiding principles for TIC use cases.

UNI/UNI Capability identifier example:

3 . UNI . RESIL

- 3 = TIC 3.0
- UNI/UNL = Universal *
- RESIL = Resiliency

* Five new capabilities added in TIC 3.0 use "UNL" rather than "UNI"

Policy Enforcement Point (PEP) Security Capabilities

Network-level security capabilities that inform technical implementation for relevant use cases.

PEP Capability identifier example:

3 . PEP . RE . DDSPR

- 3 = TIC 3.0
- PEP = Policy Enforcement Point
- RE = Resiliency (Capability Group)
- DDSPR = DDoS Protections

Unlike UNI/UNL, PEP Security Capabilities are sub-categorized into Capability Groups that map to discrete security functions like Email, Web, and Data Protection. This is new in TIC 3.0, as the program has expanded well beyond the traditional network perimeter – and now helps agencies move toward Zero Trust architectures.

PEP Capability identifiers use these abbreviations for Capability Groups:

Abbreviation	PEP Capability Group	Abbreviation	PEP Capability Group
FI	Files	**IN**	Intrusion Detection
EM	Email	**EN**	Enterprise
WE	Web	**UN**	Unified Communications and Collaboration (UCC)
NE	Networking	**DA**	Data Protection
RE	Resiliency	**SE**	Services
DO	Domain Name System (DNS)	**ID**	Identity

Table 1: PEP Capability Groups

Cloudflare Service Spotlight

By leveraging its global network, Cloudflare provides a comprehensive product portfolio spanning application performance and security, zero trust services, network services, data localization services and developer services. These solutions in particular help you accomplish your TIC 3.0 security modernization goals:

Cloudflare Access

Fast, reliable Zero Trust Network Access

Cloudflare Gateway

Cloud-native, low-latency Secure Web Gateway

Cloudflare DDoS Protection

Mitigating the biggest, most advanced attacks

Cloudflare WAF

Industry-leading web application firewall

Cloudflare Browser Isolation

High-performance remote browser isolation

Cloudflare API Gateway

Global, integrated API protection and monitoring

Cloudflare Service(s) - Mapping Overview

TIC Group		TIC Security Capability												
UNI/ UNL		3.UNI. BRECO	3.UNI. CLMAN	3.UNI. CMANA	3.UNI. IRPIH	3.UNI. INVENT	3.UNI. LPRIV	3.UNI. SADMI	3.UNI. SAUTH	3.UNI. TSYNC	3.UNI. VMANG	3.UNI. PMANA	3.UNI. AACCO	3.UNI. RESIL
		3.UNI. ETINT	3.UNI. SAWAR	3.UNI. DTDIS	3.UNI. PEPAR	3.UNI. EUSSE	3.UNI. IDMRP	3.UNI. UATRA	3 UNL. SCRMA	3.UNL. RLMAN	3.UNL. STEXE	3.UNL. CMREP	3.UNL. GPAUD	
PEP	FI	3.PEP.FI. AMALW	3.PEP.FI. CDREC	3.PEP.FI. DCHAM	3.PEP.FI. DLPRE									
	EM	3.PEP.EM. APPRO	3.PEP.EM. ASPRO	3.PEP.EM. ARCHA	3.PEP.EM. DLPRE	3.PEP.EM. DSVIE	3.PEP.EM. DSOEM	3.PEP.EM. EETRA	3.PEP.EM. MLPRO	3.PEP.EM. LCTPR	3.PEP.EM. SDENY	3.PEP.EM. PDPRO	3.PEP.EM. MFPRO	3.PEP.EM. AEPRO
		3.PEP.EM. ELABE	3.PEP.EM. UTIPP	3.PEP.EM. CFILT	3.PEP.EM. UDSOE	3.PEP.EM. EOEMA	3.PEP.EM. MCQUE	3.PEP.EM. EDRPR						
	WE	3.PEP.WE .BINSP	3.PEP.WE .ACMIT	3.PEP.WE .CDENY	3.PEP.WE .CFILT	3.PEP.WE .APROX	3.PEP.WE .DLPRE	3.PEP.WE .DRESF	3.PEP.WE .PCENF	3.PEP.WE .DCFIL	3.PEP.WE .DREPF	3.PEP.WE .BCONT	3.PEP.WE .MCFIL	3.PEP.WE .ACONT
	NE	3.PEP.NE. ACONT	3.PEP.NE. IADEN	3.PEP.NE. HCONT	3.PEP.NE. NSEGM	3.PEP.NE. MICRO	3.PEP.NE. RCONT							
	RE	3.PEP.RE. DDSPR	3.PEP.RE. EEXPS	3.PEP.RE. RDELI										
	DO	3.PEP.DO. DNSIN	3.PEP.DO. DNVAC	3.PEP.DO. DNVAD	3.PEP.DO. DNMON	3.PEP.DO. PDSER								
	IN	3.PEP.IN. EDRES	3.PEP.IN.I DPSY	3.PEP.IN. AACON	3.PEP.IN. DPLAT	3.PEP.IN. CTLMO	3.PEP.IN. NDRES							
	EN	3.PEP.EN. SOARE	3.PEP.EN. SITDE	3.PEP.EN. VPNET	3.PEP.EN. ACONT	3.PEP.EN. RDACC	3.PEP.EN. CMONI							
	UN	3.PEP.UN. IVERI	3.PEP.UN. ECOMM	3.PEP.UN. CTERM	3.PEP.UN. DLPRE	3.PEP.UN. APPRO	3.PEP.UN. MLPRO	3.PEP.UN. LCTPR	3.PEP.UN. MFPRO					
	DA	3.PEP.DA. ACONT	3.PEP.DA. PDRES	3.PEP.DA. PDTRA	3.PEP.DA. DLPRE	3.PEP.DA. DAUTE	3.PEP.DA. DLABE	3.PEP.DA. DINVE						
	SE	3.PEP.SE. ACMIT	3.PEP.SE. DLPRE	3.PEP.SE. PCENF	3.PEP.SE. MCFIL	3.PEP.SE. ACONT								
	ID	3.PEP.ID. AAUTH	3.PEP.ID. SIDEN	3.PEP.ID. EINVE	3.PEP.ID. SMANA	3.PEP.ID. BBASE	3.PEP.ID. EIAMA	3.PEP.ID. MAUTH	3.PEP.ID. CAUTH					

Legend

- Cloudflare Primary Service(s)
- Cloudflare Complementary Service(s)
- Not Available

Table 2: Cloudflare services mapping

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Backup and Recovery 3.UNI.BRECO	–	✅ All Cloudflare Products	As a cloud-based service, Cloudflare takes full responsibility for the resilience of our solutions, including backup and recovery. Our Business Service Level Agreement (SLA) commits to a level of service demonstrating 100% uptime and penalties if our service fails to meet the service level. **Important**: Cloudflare does not provide enterprise data backup and recovery solutions for other products or technologies.	Cloudflare Business Service Level Agreement
Central Log Management with Analysis 3.UNI.CLMAN	–	✅ All Cloudflare Products	All Cloudflare solutions generate detailed logs for debugging, tuning configurations, and creating analytics, especially when combined with logs from other sources such as your application server. With Cloudflare's Logpush service, you can configure the automatic export of Zero Trust logs to third-party storage destinations or to Security Information and Event Management (SIEM) tools. Once exported, your team can analyze and audit the data as needed. **Important**: Cloudflare does not provide SIEM or enterprise log management solutions.	Cloudflare Logs Cloudflare Logpush Cloudflare Audit Logs Cloudflare Web Analytics
Configuration Management 3.UNI.CMANA	–	✅ All Cloudflare Products	Cloudflare provides a centralized dashboard to make it easy to manage and configure our cloud-based offerings. Audit logs summarize the history of changes made within your Cloudflare account, including account level actions like login and zone configuration changes. **Important**: Cloudflare does not offer an Enterprise Configuration Management (ECM) solution or Configuration Management Database (CMDB) for other products or technologies.	Cloudflare Rules Cloudflare Logs Cloudflare Audit Logs
Incident Response Planning and Incident Handling 3.UNI.IRPIH	✅ Cloudflare Security Operations Center-as-a-Service	✅ All Cloudflare Products	Cloudflare SOC-as-a-Service monitors your environment for security threats and potential operational disruptions, performs deep analysis to identify attack vectors, and helps you implement countermeasures to mitigate future incidents. And Cloudflare's Emergency Hotline is there to help you respond to DDoS, ransomware, identity or access, network, web and application attacks. **Important**: This TIC capability is a comprehensive people and process control that requires agency responsibilities.	Cloudflare Security Operations Center-as-a-Service Cloudflare Under Attack Hotline
#5 of 25 **Inventory** 3.UNI.INVENT	–	✅ Cloudflare Security Center	Cloudflare Security Center scans known assets, identifies unknown assets, and detect rouge assets to map the attack surface and identify potential vulnerabilities. **Important**: Cloudflare does not provide enterprise asset management or configuration management database (CMDB) solutions.	Cloudflare Security Architecture

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Least Privilege 3.UNI.LPRIV	✅ Cloudflare Security Access Service Edge (SASE) and Security Service Edge (SSE) services	✅ All Cloudflare Products	Cloudflare SASE & SSE services provide context-based, least privilege access on a per-resource basis rather than at the network-level. This protects critical resources and sensitive data by implementing app-specific, least-privilege access for external users based on Zero Trust principles. Cloudflare also supports API tokens for granular administrative privileges via APIs.	Cloudflare Security Architecture
Secure Administration 3.UNI.SADMI	–	✅ All Cloudflare Products	Cloudflare secures its administrative dashboard with Multi Factor Authentication (MFA) and Transport Layer Security (TLS). You can also securely manage Cloudflare with API tokens that provide granular permissions.	Account Security
Strong Authentication 3.UNI.SAUTH	✅ Cloudflare Access Cloudflare API Gateway	–	Cloudflare Access supports authenticating via identity providers with strong, Multi-Factor Authentication (MFA). It checks granular context like identity and device posture for every request to provide fast, reliable access across your business. Cloudflare API Gateway supports Mutual TLS (mTLS) authentication using client certificates. API Gateway's JWT Validation cryptographically verifies incoming JWTs before they are passed to the API origin. **Important**: Cloudflare is not an Identity Provider (IdP), and does not provide enterprise-wide Identity and Access Management (IAM) capabilities for other products or technologies.	Enforce MFA
Time Synchronization 3.UNI.TSYNC	✅ Cloudflare Time Services	✅ All Cloudflare Products	Cloudflare Time Services supports the Network Time Protocol (NTP) and Network Time Security (NTS). We also support Google Roughtime (in beta). Cloudflare also synchronizes time across its entire platform so that all products and services measure time accurately.	Cloudflare Time Services

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Vulnerability Management 3.UNI.VMANG	–	✅ Cloudflare Security Center Cloudflare Web Application Firewall (WAF)	Cloudflare Security Center offers attack surface management (ASM) that inventories IT assets, enumerates potential security issues, controls phishing and spoofing risks, and enables security teams to investigate and mitigate threats. Cloudflare WAF offers Cloudflare Managed Rules, updated frequently, to help defend against new vulnerabilities and reduce false positives. Additional vulnerabilities are covered with OWASP Core Ruleset, and Exposed Credential Check. Also, since Cloudflare is a cloud-based service, we take full responsibility for service resilience, including vulnerability management, of our SaaS products and services according to our Business Service Level Agreement (SLA). **Important**: Cloudflare does not offer an enterprise Vulnerability Management (VM) solution for other products or technologies.	Reference architecture Cloudflare Business Service Level Agreement
Patch Management 3.UNI.PMANA	–	✅ All Cloudflare Products	Cloudflare is a cloud-based service, so we take full responsibility for service resilience, including patch management, of our SaaS products and services according to our Business Service Level Agreement (SLA). **Important**: Cloudflare does not offer an enterprise Patch Management solution for other products or technologies.	Reference architecture Cloudflare Business Service Level Agreement
Auditing and Accounting 3.UNI.AACCO	–	✅ All Cloudflare Products	Cloudflare provides logging and analytics both in the Cloudflare dashboard and to external solutions for centralized auditing and reporting. **Important**: This TIC capability is a comprehensive people and process control that requires agency responsibilities.	Reference architecture
Resilience 3.UNI.RESIL	✅ Cloudflare Zero Trust Cloudflare Network Services Cloudflare Application Services	✅ All Cloudflare products	Cloudflare's Zero Trust security solutions, network and applications services help ensure mission operations, even under adverse conditions like DDoS attacks, DNS exploitation, web cache poisoning and other attack vectors. We build security and resilience into all of our cloud-delivered services, backed by our FedRAMP authorization and other service certifications found on Cloudflare's Trust Hub.	Reference architecture The Cloudflare Trust Hub

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Enterprise Threat Intelligence 3.UNI.ETINT	✅ Cloudforce One	✅ All Cloudflare products	Cloudforce One is Cloudflare's packed security intelligence, tools, and operations to make security teams smarter, more responsive, and more secure. We gather unique threat intelligence from our vast global network, leveraging Cloudflare's team of world-class researchers that analyze and refine security data into actionable threat intelligence used by all Cloudflare security products. Our API-driven threat feeds easily integrate via STIX/TAXII into SOC workflows and security products like SIEM/SOAR, EDR/XDR, TIP platforms, firewalls, or security analytics. Our threat intelligence automatically protects Cloudflare customers, automatically fed into our Zero Trust suite, Magic Firewall, WAF and API Gateway.	Threat intelligence APIs
Situational Awareness 3.UNI.SAWAR	✅ Cloudflare API Gateway Cloudflare Web Application Firewall (WAF) Cloudflare Bot Management Cloudflare DDoS	✅ All Cloudflare products	Cloudflare maintains situational awareness throughout our solutions by baselining traffic and patterns across sites to detect anomalies and suspicious behavior. For example: Cloudflare Bot Mgmt uses baselines to detect the anomalies typical of non-human traffic. Cloudflare API Gateway builds a baseline to provide recommendations on rate limiting per endpoint to protect against abuse. Cloudflare WAF uses machine learning to detect variations designed to bypass WAF and uses this data to enhance the machine learning models used. Cloudflare Logpush service exports logs to third-party storage destinations or to Security Information and Event Management (SIEM) tools for analysis and situational awareness.	Reference architecture Logpush integration
Dynamic Threat Discovery 3.UNI.DTDIS	✅ Cloudflare API Gateway Cloudflare Web Application Firewall (WAF) Cloudflare Bot Management	✅ All Cloudflare products	Cloudflare discovers threats dynamically through heuristics, machine learning, and baselining to spot threat actor tactics and techniques like volumetric abuse, credit card skimming, credential stuffing, and so forth.	Reference architecture
Policy Enforcement Parity 3.UNI.PEPAR	✅ All Cloudflare products	–	Cloudflare applies consistent, granular policies across Cloudflare Access, API gateway, Bot Mgmt, Gateway, Magic Firewall, and WAF across endpoints from a single user interface.	Manage Cloudflare Zero Trust policies

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Effective Use of Shared Services 3.UNI.EUSSE	✅ All Cloudflare products	–	Cloudflare products use shared services such as threat intelligence from both internal and external sources to enhance security capabilities and identify malicious actors and activity. Cloudflare leverages intelligence and data from our global network, as well as machine learning model outputs based on this data to create attributes like threat score, bot score, and WAF attack score that can be used in security policies. A logical level of multi-tenancy is built into the platform and achieved at the request level. Ownership and Access Control Lists (ACLs) are assigned to a request at the edge, and users can create and control multiple tenants that use identical Cloudflare services, but will not have any of their data or traffic cross-pollinated while doing so.	Reference architecture
Integrated Desktop, Mobile, and Remote Policies 3.UNI.IDMRP	✅ All Cloudflare products	–	Cloudflare WAF, Bot Mgmt, and API Gateway policies apply to all HTTP requests going to origin serves regardless of source. Cloudflare Secure Access Service Edge (SASE_ services like Cloudflare Access and Gateway can apply policies based on device posture against any onboarded application or HTTP/network destination, regardless of the user's geolocation.	Reference architecture
User Awareness and Training 3.UNI.UATRA	–	✅ All Cloudflare products	Cloudflare provides security architects, analysts, and administrators with clear documentation, reference architectures, and educational videos and webinars to help ensure they understand how to implement, configure, use, and monitor Cloudflare services. **Important**: Cloudflare is a not a learning management system, and does not provide education or training for end users.	Reference architecture Learning paths
Supply Chain Risk Management 3 UNL.SCRMA	–	✅ All Cloudflare products	"Cloudflare helps you manage a wide range of supplier risks, from Software to Cybersecurity to Information and Communications Technology (ICT) supply chain risks. For example, Cloudflare Zero Trust solutions help you manage third-party access and enforce least privilege access by users, devices, or workloads, and Cloudflare Network Services help implement micro-segmentation to protect against exploited supplier networks from affecting yours. We can effectively hide the internal applications from the Internet, protecting them from attackers seeking to exploit unpatched software vulnerabilities. And Cloudflare DNS filtering can block command and control attacks, which may be hidden in software updates by blocking the DNS request required to establish this unauthorized connection. Important: Cloudflare is a not a supply chain risk management platform, but it helps you implement important controls to manage supply chain risks.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Universal (UNI/UNL) Security Capabilities

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Resource Lifecycle Management 3.UNL.RLMAN	–	–	Cloudflare is not a resource lifecycle management platform.	–
Security Test and Exercise 3.UNL.STEXE	–	–	Cloudflare is not a penetration testing or cyber range platform.	–
Continuous Monitoring Reporting 3.UNL.CMREP	–	✅ Cloudflare Security Access Service Edge (SASE) and Security Service Edge (SSE) services	Cloudflare SASE and SSE services provide threat data, tooling, and access to industry experts. In addition to “requests for information” (RFIs) to experts, within Security Center, users can see analytics, events, reports, and use the ‘Investigate’ tab for querying current and historical threat data on IPs, ASNs, URLs, and domains. Brand protection can be enabled to search for new domains that may be attempting to impersonate customer’s brand. Cloudflare also provides real time log streams to agency SIEMs to facilitate continuous monitoring. **Important**: This TIC capability is a comprehensive people and process control that requires agency responsibilities."	Security reports
Governance and Policy Auditing 3.UNL.GPAUD	–	✅ Cloudflare Security Access Service Edge (SASE) and Security Service Edge (SSE) services Cloudflare Data Localization Suite	Cloudflare can help with the policy enforcement. Governance and definition is customer’s responsibility. Policies can be applied across multiple products/services from a single dashboard - WAF, API gateway, Bot Management, and Access and Gateway policies. Cloudforce One specifically enables users to test access policies, helping them determine whether or not unauthorized users would have access to a given resource. Cloudflare Data Localization Suite empowers users to more effectively comply with data residency and governance laws **Important**: Cloudflare is not an enterprise Governance, Risk, and Compliance (GRC) solution.	

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Files (FI) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Anti-malware 3.PEP.FI.AMALW	✅ Cloudflare DNS Cloudflare Gateway Cloudflare Web Application Firewall (WAF) Cloudflare Email Security	–	Cloudflare solutions help detect, analyze and stop malware. Cloudflare DNS stops users from accessing sites known to distribute malware. Malicious uploads detection scans uploaded content for malicious signatures, such as malware. Cloudflare Gateway allows admins to scan files for malware as users upload or download them, and can quarantine files to protect against zero-day vulnerabilities. Cloudflare WAF Content Scanning can stops malicious files from reaching web servers. Cloudflare Email Security uses structural analysis, sentiment analysis, and trust graphs to identify and stop malware from reaching end users' mailboxes.	Prevent malware uploads
Content Disarm and Reconstruction 3.PEP.FI.CDREC	–	✅ Cloudflare Browser Isolation Cloudflare Page Shield	Cloudflare Browser Isolation service is built on Chromium, an open-source browser that helps provide a safer, faster, and more stable way for all users to experience the web. Cloudflare's service initiates headless Chromium browsers that proxy connections between the user and the origin server, creating an environment where content can be disarmed. Cloudflare Page Shield can detect malicious Javascript files and alert customers. Content security policies can be applied to restrict script sources and connection destinations. **Important**: Cloudflare does not provide content reconstruction, sandboxing, or malware analytics solutions. Also, Cloudflare Page Shield is not FedRAMP authorized at this time.	Isolation policies Page Shield
Detonation Chamber 3.PEP.FI.DCHAM	–	✅ Cloudflare Browser Isolation	Cloudflare Browser Isolation creates an environment that satisfies the criteria of a 'protected and isolated execution environment'. While the remote browser does not explicitly scan for threats, all traffic that goes through the remote browser is still subject to the organization's gateway rules, which include identifying websites that are known security threats, and our Uploaded Content Scanning applicable only to files in plain text in the response body. **Important**: Cloudflare does not provide content reconstruction, sandboxing, or malware analytics solutions.	Isolation policies
Data Loss Prevention 3.PEP.FI.DLPRE	✅ Cloudflare Data Loss Prevention (DLP)	✅ All Cloudflare products	Cloudflare solutions enable DLP profiles that use regular expression (regex) patterns in HTTP/S traffic, SaaS applications, and APIs to identify and alerts on sensitive data in transit or at rest. You can also apply these DLP profiles to Microsoft 365 Outlook clients through an add-in.	Data Loss Prevention

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Email (EM) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Anti-phishing Protections 3.PEP.EM.APPRO	✅ Cloudflare Email Security	–	Cloudflare Email Security uses globally distributed sensors and comprehensive attack analytics to identify phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Cloudflare Email Security allows customers to take preemptive action against targeted phishing, including malware, spoofing attacks, payload-less Business Email Compromise attacks, supply chain phishing, and other advanced threats. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Cloudflare Email Security PhishGuard Email Security Policies
Anti-spam Protections 3.PEP.EM.ASPRO	✅ Cloudflare Email Security	–	Cloud Email Security email security detects and categorizes spam messages, stopping them before they reach the recipient. It provide a detailed analysis of the message content and the reasoning behind its categorization decisions. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Cloudflare Email Security Email Security Policies
Authenticated Received Chain 3.PEP.EM.ARCHA	✅ Cloudflare Email Security	–	Cloud Email Security enables downstream entities to accept alternative authentication if sent through a forwarding service or equivalent intermediary. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Cloudflare Email Security Email Security Policies
Data Loss Prevention 3.PEP.EM.DLPRE	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare Email Security	–	Cloudflare DLP and Cloudflare Email Security work together to scan outbound emails in Microsoft 365 environments. Outbound Data Loss Prevention integrates with your inbox, and it proactively monitors your email to prevent unauthorized data leaks. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time, and Outbound DLP works only with Microsoft 365.	Outbound DLP

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Email (EM) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Domain Signature Verification for Incoming Email 3.PEP.EM.DSVIE	✅ Cloudflare DMARC Management (beta) Cloudflare DNS	✅ Cloudflare Email Security	Cloudflare DMARC Management (beta) helps you track every source that is sending emails from your domain and review Domain-based Message Authentication Reporting and Conformance (DMARC) reports for each source. DMARC reports will help you understand if messages sent from your domain are passing DMARC authentication, DomainKeys Identified Mail (DKIM) authentication, and Sender Policy Framework (SPF) policies. **Important**: Cloudflare Email Security is not FedRAMP authorized and Cloudflare DMARC Management is in beta at this time.	Cloudflare DMARC Management (beta)
Domain Signatures for Outgoing Email 3.PEP.EM.DSOEM	–	✅ Cloudflare DNS	Cloudflare DNS can host records that enable DMARC (including DMARC reporting), ARC, DKIM, and SPF for a zone. **Important**: Cloudflare does not handle outbound email directly.	Cloudflare DMARC Management (beta)
Encryption for Email Transmission 3.PEP.EM.EETRA	✅ Cloudflare Email Security	–	Cloudflare Email Security uses opportunistic TLS by default. You can enforce TLS for all communications, rejecting email that lacks TLS. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Partner Domains TLS
Malicious Link Protections 3.PEP.EM.MLPRO	✅ Cloudflare Email Security	–	Cloudflare Email Security can detect malicious links within emails and disable them when the user views it. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Detection settings
Link Clickthrough Protections 3.PEP.EM.LCTPR	✅ Cloudflare Email Security	✅ Cloudflare Browser Isolation	Cloudflare Email Security can isolate suspicious email links so that they load in an isolated browser and provide interstitial pages that warn the user of potentially dangerous content within the link. Email Link Isolation rewrites links in emails and opens them in a browser tab where all page contents are fetched and rendered on a remote server. When this feature is enabled, any malware that might be present in a web page or email link is isolated at the server level, and will not infect and compromise the client network at the endpoint. . **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Link actions

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Email (EM) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Sender Denylisting 3.PEP.EM.SDENY	✅ Cloudflare Email Security	–	Cloudflare Email Security supports sender denylisting. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time. "	Block lists
Post-Delivery Protections 3.PEP.EM.PDPRO	✅ Cloudflare Email Security	–	Cloudflare Email Security supports post-delivery protections like email quarantine and data link protections. Phishing retro scan can identify threats that have already reached your end users. When using the API configuration, Cloudflare Email Security can retract messages manually or configure automatic retractions to move messages matching certain dispositions to specific folders within a user's mailbox. You can also enable Post Delivery Response and Phish Submission Response to re-evaluate messages previously delivered against new information gathered by Email Security. Scanned emails that were previously delivered and now match this new phishing information will be retracted. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Retract settings
Malicious File Protections 3.PEP.EM.MFPRO	✅ Cloudflare Email Security	–	Cloudflare Email Security performs a detailed risk-based analysis when identifying potential threats. Analysis techniques include using AI and multiple machine learning models. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Detection settings
Adaptive Email Protections 3.PEP.EM.AEPRO	✅ Cloudflare Email Security	–	Cloudflare Email Security performs a detailed risk-based analysis when identifying potential threats. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Detection settings
Email Labeling 3.PEP.EM.ELABE	✅ Cloudflare Email Security	–	Cloudflare Email Security can automatically tag incoming emails based on the identified security threat. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Dispositions
User Tipping 3.PEP.EM.UTIPP	✅ Cloudflare Email Security	–	Cloudflare Email Security enables users to report suspicious emails or links within emails as potential threats. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Phish submissions

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Email (EM) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Content Filtering 3.PEP.EM.CFILT	✅ Cloudflare Email Security	–	Cloudflare Email security blocks and isolates phishing threats, including email-borne malware, business email compromise, and multi-channel (link-based) attacks. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Enhanced detections
User Digital Signatures for Outgoing Email 3.PEP.EM.UDSOE	–	–	Cloudflare Email Security does not support digital signatures for outbound emails.	–
Encryption for Outgoing Email 3.PEP.EM.EOEMA	–	–	Cloudflare Email Security does not support encryption for outbound emails.	–
Mail Content Query 3.PEP.EM.MCQUE	✅ Cloudflare Email Security	–	Cloudflare Email Security supports search and discovery across all managed inboxes. Fielded Search presents you with fields where you can enter search terms, and Freeform Search has one search field where you can construct your own search query **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Email Security search
Email Domain Reputation Protections 3.PEP.EM.EDRPR	✅ Cloudflare Email Security	–	Cloud Email Security supports domain reputation protections. Phishguard and Cloudforce One also provide these services to the end user. **Important**: Cloudflare Email Security is not FedRAMP authorized at this time.	Email Security

Cloudflare Service Mapping Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Web (WE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Break and Inspect 3.PEP.WE.BINSP	✅ Cloudflare Web Application Firewall (WAF) Cloudflare Spectrum Cloudflare Gateway Cloudflare SSL/TLS Certificates	–	Cloudflare Web Application Firewall (WAF) proxies connections between client and server, so it can decrypt (break), inspect, and then re-encrypt web traffic. Cloudflare Spectrum is a reverse proxy that extends Cloudflare protections to all TCP/UDP applications. Cloudflare Gateway (Secure Web Gateway) can conduct break and inspect to enforce L4 and L7 HTTP and DNS rules.	Decrypt payload content
Active Content Mitigation 3.PEP.WE.ACMIT	✅ Cloudflare Gateway Cloudflare Browser Isolation Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway blocks malicious active content through AV scanning or Cloudflare Browser Isolation technology to execute, process, and render untrusted or malicious active content on our edge network far away from the customer's devices and networks. Sensitive data detection alerts on responses containing sensitive data from webapps or APIs. Cloudflare Web Application Firewall (WAF) scans for malicious file uploads that may include malware or viruses and can block upload.	Malicious uploads detection Browser Isolation
Certificate Denylisting 3.PEP.WE.CDENY	✅ Cloudflare TLS/SSL Certificates	✅ All Cloudflare products	All Cloudflare products support Online Certificate Status Protocol (OCSP) and certificate revocation lists (CRLs).	Mutual TLS
Content Filtering 3.PEP.WE.CFILT	✅ Cloudflare Gateway	–	Cloudflare Gateway (Secure Web Gateway) allows administrators to create DNS and HTTP filtering policies to block or allow requests based on various selectors such as destination host, URL, URL query, URL path, HTTP method, HTTP response, uploaded/downloaded file extension, uploaded/downloaded MIME type, content categories, and applications.	Secure Web Gateway
Authenticated Proxy 3.PEP.WE.APROX	✅ Cloudflare Access Cloudflare API Gateway	–	Cloudflare Access supports authenticating via supported identity providers with a robust suite of device and security posture checks. Cloudflare API Gateway supports Mutual TLS (mTLS) authentication using client certificates to ensure traffic between client and server is bidirectionally secure and trusted. mTLS also allows requests that do not authenticate via an identity provider, such as Internet-of-things (IoT) devices, to demonstrate they can reach a given resource. API Gateway's JWT Validation stops JWT replay attacks and JWT tampering by cryptographically verifying incoming JWTs before they are passed to your API origin. JWT Validation will also stop requests with expired tokens or tokens that are not yet valid.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Web (WE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Data Loss Prevention 3.PEP.WE.DLPRE	✅ Cloudflare Gateway Cloudflare API Gateway Cloudflare Web Application Firewall (WAF)	–	Cloudflare API Gateway can flag endpoints returning sensitive data on API request calls. DNS and HTTP rules can be created in Cloudflare Gateway that block or allow traffic based on various criteria (e.g. upload MIME type) that can control the flow of data. Cloudflare Web Application Firewall (WAF) has Sensitive Data Detection rules that monitor and flag the download of specific sensitive data — for example, financial and personally identifiable information.	Reference architecture
Domain Resolution Filtering 3.PEP.WE.DRESF	✅ Cloudflare Gateway	✅ Cloudflare DNS	Cloudflare Gateway supports both DNS over HTTPS (DoH) and DNS over TLS (DoT). and inspects all DNS queries, including DoH.	DNS policies
Protocol Compliance Enforcement 3.PEP.WE.PCENF	✅ Cloudflare Gateway Cloudflare Magic Firewall Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway networking rules and Cloudflare Magic Firewall can enforce the use of specific protocols and ports against L3 destinations. Cloudflare WAF rules block requests based on many different HTTP attributes and protocol violations like invalid HTTP Request Line or Content-Length HTTP header issues.	Reference architecture
Domain Category Filtering 3.PEP.WE.DCFIL	✅ Cloudflare Gateway	–	Cloudflare Gateway (Secure Web Gateway) policies can inspect DNS, Network, HTTP, and Egress traffic. DNS policies inspect DNS queries. You can block domains and IP addresses from resolving on your devices. Network policies inspect individual TCP/UDP/GRE packets. You can block access to specific ports on your origin server, including non-HTTP resources. HTTP policies inspect HTTP requests. You can block specific URLs from loading, not just the domain itself. Egress policies inspect traffic to assign egress IP addresses unique to your organization. Resolver policies inspect DNS queries to enable resolution by custom authoritative nameservers.	Domain categories App types

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Web (WE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Domain Reputation Filtering 3.PEP.WE.DREPF	✅ Cloudflare Gateway Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway can filter requests based on low reputation scores like newly-seen domains, Domain Generation Algorithm (DGA) domains, and custom domain lists. Cloudflare WAF can block based on threat score and domain reputation.	Secure Web Gateway
Bandwidth Control 3.PEP.WE.BCONT	✅ Cloudflare Gateway Cloudflare Web Application Firewall (WAF)	–	Rate Limiting allows customers to limit traffic to a domain or endpoint based on different criteria. Once the rate is exceeded, the WAF will take action all requests during the selected duration before the counter resets. Customers also have the option to throttle request above the maximum configured rate (sliding window effect).	Secure Web Gateway
Malicious Content Filtering 3.PEP.WE.MCFIL	✅ Cloudflare Gateway Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway can block malicious active content utilizing AV scanning or by using browser isolation technology to execute, process, and render untrusted or malicious active content on our edge network far away from the customer's devices and networks. Uploaded Content Scanning scans for malicious file uploads that may include malware or viruses and can block upload.	Secure Web Gateway
Access Control 3.PEP.WE.ACONT	✅ Cloudflare Access	–	Cloudflare Access supports authenticating via one of the supported identity providers. Identity-based policies can be created to allow specific users or groups of users to access an internal application or cloud-based application.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Networking (NE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Access Control 3.PEP.NE.ACONT	✅ Cloudflare Access Cloudflare Gateway Cloudflare Magic Firewall Cloudflare API Gateway	–	Cloudflare can support access controls for L3 traffic via Cloudflare Access and Cloudflare Gateway policies, as well as Cloudflare Magic Firewall service. Cloudflare Gateway network policies not only specify IP and Protocols, but can include Identity and Device Posture requirements, which serve as access control measures for L3 destinations. Private IP applications that are onboarded to access also support identity-based policies. Cloudflare Magic Firewall is a network-level firewall that allows Magic Transit customers to control network-based traffic with firewall rules. Cloudflare API Gateway supports Mutual TLS (mTLS) authentication and uses client certificates to ensure traffic between client and server is bidirectionally secure and trusted. mTLS also allows requests that do not authenticate via an identity provider, such as Internet-of-things (IoT) devices, to demonstrate they can reach a given resource. API Gateway's JWT Validation stops JWT replay attacks and JWT tampering by cryptographically verifying incoming JWTs before they are passed to your API origin. JWT Validation will also stop requests with expired tokens or tokens that are not yet valid.	Reference architecture
Internet Address Denylisting 3.PEP.NE.IADEN	✅ Cloudflare Gateway Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway can prevent users from accessing destinations that have been properly identified within Secure Web Gateway (SWG) network policies. Cloudflare WAF allows for denylisting based on L3, L4, and L7 criteria.	Reference architecture
Host Containment 3.PEP.NE.HCONT	✅ Cloudflare Access Cloudflare Gateway	–	Cloudflare Access and Gateway policies can be changed to revoke user access to specific applications. Cloudflare Zero Trust enables policies that use device posture signals from the Cloudflare WARP client or from third-party endpoint security providers. When device posture checks are configured, they are permitted to access protected applications or network resources only if they have a managed or healthy device. Under the "My Team" section in the ZT dashboard, customers can identify specific users and devices that have access to the environment and revoke any and all authorized sessions.	Reference architecture Cloudflare Zero Trust Device posture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Networking (NE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Network Segmentation 3.PEP.NE.NSEGM	✅ Cloudflare Gateway	–	Cloudflare supports network segmentation through SSE services including Cloudflare WARP, Cloudflare Tunnel and Cloudflare Gateway. Cloudflare Tunnel and WARP proxy IP addresses from the origin server or from something that has L3 connectivity to the origin server, and has a default-deny policy against any non-connector traffic attempting to access the origin server. This also provides access to the resource, rather than the subnet that contains the resource, preventing lateral movement across a network. Cloudflare Gateway policies can be used to apply 5-tuple rules towards L3 destinations. Cloudflare Magic Firewall also allows users to create similar policies across their WAN.	Reference architecture
Micro-segmentation 3.PEP.NE.MICRO	✅ Cloudflare Security Service Edge (SSE) Cloudflare Magic Firewall	–	In addition to the network segmentation capabilities outlined above with Tunnel and Gateway, Cloudflare also provides Virtual Networks which can create logically-defined subnets that can contain overlapping IP addresses. Users can toggle between these vNets using their device client, Cloudflare WARP.	Reference architecture Cloudflare Tunnel
Resource Containment 3.PEP.NE.RCONT	✅ Cloudflare Gateway	–	Server-to-server communication can be managed and revoked based on how the communication was created - either by revoking the mTLS certificate or by creating L3 policies that can target the IP ranges specified by the WARP connector.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Resiliency (RE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Distributed Denial of Service Protections 3.PEP.RE.DDSPR	✅ Cloudflare Network Services Cloudflare DDoS Cloudflare Magic Transit Cloudflare Spectrum Cloudflare Web Application Firewall (WAF)	–	Cloudflare's global network leverages Anycast and has every service running on every server so users are always routed to their closest location. This inherently also protects against DDoS attacks by maximizing the surface area to absorb attacks. Additionally, Cloudflare offers several products that mitigate L3, L4, and L7 type DDoS Attacks. Cloudflare can provide 'always-on' DDoS protection.	Reference architecture Cloudflare Rate Limiting
Elastic Expansion 3.PEP.RE.EEXPS	✅ All Cloudflare Products	–	Cloudflare offers SaaS for performance, security, reliability, and developer services. Cloudflare spans across 310 cities in 120+ countries with 13,000 networks directly connected, including every major ISP, cloud provider, and enterprise. Inherently, Cloudflare scales as needed across its global network and infrastructure autonomously as needed without any intervention from customers.	Reference architecture
Regional Delivery 3.PEP.RE.RDELI	✅ All Cloudflare Products	–	Cloudflare regional services accommodate regional restrictions while still using the Cloudflare global edge network.	Reference architecture
Domain Name Sinkholing 3.PEP.DO.DNSIN	✅ Cloudflare Gateway	✅ Cloudflare DNS	Cloudflare Gateway allows administrators to create DNS filtering policies to "override" specific domain names. The override will forward all requests to a given destination to another destination the administrator sets. Sinkholes can be created on-demand, as a service, to monitor hosts infected with malware and prevent them from communicating with command-and-control (C2) servers. After creating a sinkhole, an IP will be returned which can be used with DNS products like Cloudflare Gateway to route web requests to safe sinkholes (and away from C2 servers). Sinkholes can be used to intercept SMTP traffic.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

DNS (DO) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Domain Name Sinkholing 3.PEP.DO.DNSIN	✅ Cloudflare Gateway	✅ Cloudflare DNS	Cloudflare Gateway allows administrators to create DNS filtering policies to "override" specific domain names. The override will forward all requests to a given destination to another destination the administrator sets. Sinkholes can be created on-demand, as a service, to monitor hosts infected with malware and prevent them from communicating with command-and-control (C2) servers. After creating a sinkhole, an IP will be returned which can be used with DNS products like Cloudflare Gateway to route web requests to safe sinkholes (and away from C2 servers). Sinkholes can be used to intercept SMTP traffic.	Reference architecture
Domain Name Verification for Agency Clients 3.PEP.DO.DNVAC	✅ Cloudflare DNS Cloudflare Gateway	–	Cloudflare helps agency devices verify whether or not the domain names they're navigating to are accurate and legitimate entities. If Cloudflare nameservers are being used, Cloudflare can accomplish this via its Global DNS service. Gateway DNS policies also provides for domain name verification.	Reference architecture
Domain Name Validation for Agency Domains 3.PEP.DO.DNVAD	✅ Cloudflare DNS Cloudflare Gateway	–	Cloudflare helps agency clients verify whether or not the domain names they're navigating to are accurate and legitimate entities. If Cloudflare nameservers are being used, Cloudflare can accomplish this via its Global DNS service. Gateway DNS policies also provides for domain name verification. **Important**: The Cybersecurity and Infrastructure Security Agency (CISA) uses Cloudflare to provide Registry and Protective DNS services that enhance resilience and simplify security operations for .gov domain users.	Reference architecture
Domain Name Monitoring 3.PEP.DO.DNMON	✅ Cloudflare DNS	–	Cloudflare DNS provides Audit logs summarize the history of changes made within your Cloudflare account. Audit logs include account level actions like login, as well as zone configuration changes. Audit logs also integrate with Security Information and Event Management (SIEM) solutions.	Analytics and logs Review audit logs
CISA's Protective DNS Service 3.PEP.DO.PDSER	✅ Cloudflare DNS	–	Cloudflare DNS filtering integrates with CISA Protective DNS service. **Important**: The Cybersecurity and Infrastructure Security Agency (CISA) uses Cloudflare to provide Protective DNS services that enhance resilience and simplify security operations for .gov domains.	Set up DNS filtering

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Intrusion Detection (IN) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Endpoint Detection and Response 3.PEP.IN.EDRES	–	✅ Cloudflare Access Cloudflare Gateway	Cloudflare Zero Trust enforces policies that rely on additional signals from the WARP client or from third-party endpoint security providers. When device posture checks are configured, users can only connect to a protected application or network resource if they have a managed or healthy device. **Important**: Cloudflare does not provide comprehensive Endpoint Detection and Response (EDR) capabilities, but integrates with leading vendors in this space.	Device posture
Intrusion Detection and Prevention Systems 3.PEP.IN.IDPSY	–	✅ Cloudflare Magic Firewall	Cloudflare Magic Firewall includes an IDS that takes advantage of the threat intelligence powered by our global network and extends the capabilities of the Cloudflare Firewall to monitor and protect your network from malicious actors. **Important**: Cloudflare does not offer IPS capabilities today.	Enable IDS
Adaptive Access Control 3.PEP.IN.AACON	–	✅ Cloudflare Access Cloudflare Gateway	Cloudflare Access can factor in additional context to access control decisions through security posture requirements for users/groups, and individualized user risk scores. Cloudflare leverages intelligence and data from it's global network as well as machine learning model outputs based on this data to create attributes like threat score, bot score, and WAF attack score that can be used in security policies to limit access to origin servers.	Reference architecture
Deception Platforms 3.PEP.IN.DPLAT	–	–	Cloudflare is not a deception platform or decoy environment.	–

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Intrusion Detection (IN) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Certificate Transparency Log Monitoring 3.PEP.IN.CTLMO	✅ Cloudflare TLS/SSL Certificates	–	Cloudflare can perform comprehensive Certificate Transparency Log Monitoring (CTLM) via its SSL/TLS certificate management.	Cloudflare SSL/TLS
Network Detection and Response 3.PEP.IN.NDRES	–	✅ Cloudflare Access Cloudflare Gateway Cloudflare Magic Firewall Cloudflare Web Application Firewall (WAF)	Cloudflare can log all network data that occurs across its edge, which can assist in the detection and remediation of malicious activity. In context of Zero Trust, this means analyzing local L3 network traffic and applications explicitly onboarded to Cloudflare Access; this analysis is performed via Gateway and the Device Client. Magic Firewall, WAF, and Security Analytics provides for logging capabilities at the edge using L3-L7 criteria	Reference architecture Cloudflare WARP Cloudflare Security Analytics

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Enterprise (EN) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Security Orchestration, Automation, and Response 3.PEP.EN.SOARE	–	✅ Cloudflare Application Security	Cloudflare Application Security solutions can detect threats or vulnerabilities in web and SaaS applications and recommend remediation actions, and it integrates via API with SIEM and SOAR for additional analysis and response automation. **Important**: Cloudflare is not a Security Orchestration, Automation and Response (SOAR) platform.	Reference architecture
Shadow Information Technology Detection 3.PEP.EN.SITDE	✅ Cloudflare API Gateway	–	Cloudflare API Gateway leverages machine learning to discovers API endpoints in use by an organization and prevents shadow APIs. It extracts HTTP headers from user traffic and associates them with applications.	Reference architecture
Virtual Private Network 3.PEP.EN.VPNET	✅ Cloudflare Access	–	Cloudflare Access provides Zero Trust Network Access (ZTNA). the modern approach to secure remote access that replaces legacy VPN technologies. It verifies context like identity and device posture to secure access across your entire environment.	Cloudflare Access
Application Container 3.PEP.EN.ACONT	–	✅ Cloudflare Workers	Cloudflare Workers deploys serverless code instantly on Cloudflare's global edge for exceptional performance, reliability, and scale. Workers handles each request for your domain at a Cloudflare location close to the end user, essentially making your code "run everywhere." With Cloudflare Workers, you can build "serverless" applications that rely entirely on web APIs, and strengthen web security with custom rules, filters, authentication and authorization mechanisms. **Important**: Cloudflare does not offer traditional Application Container services. Cloudflare Workers is the new way to securely distribute serverless code around the globe.	Cloudflare Workers
Remote Desktop Access 3.PEP.EN.RDACC	–	✅ Cloudflare Access	Cloudflare can proxy existing solutions (SSH, VNC) through a browser and manage RDP connections by onboarding them as a Cloudflare Access application. **Important**: Cloudflare does not provide RDP services.	Cloudflare Access
Costs Monitoring 3.PEP.EN.CMONI	–	✅ Cloudflare Plans	Cloudflare Plans are custom pricing packages that help agencies manage and control Cloudflare's solution costs through predictable pricing. **Important**: Cloudflare does not monitor costs for any other technology.	Cloudflare Account Management and Billing

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Unified Comms (UN) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Identity Verification 3.PEP.UN.IVERI	–	–	Cloudflare does not address identity verification inside Unified Communications products.	–
Encrypted Communication 3.PEP.UN.ECOMM	–	–	Cloudflare does not encrypt Unified Communication sessions.	–
Connection Termination 3.PEP.UN.CTERM	–	–	Cloudflare does not terminate connections within Unified Communications products.	–
Data Loss Prevention 3.PEP.UN.DLPRE	–	–	Cloudflare does not address data loss inside Unified Communications products.	–
Anti-phishing Protections 3.PEP.UN.APPRO	–	–	Cloudflare does not address phishing inside Unified Communications products.	–
Malicious Link Protections 3.PEP.UN.MLPRO	–	–	Cloudflare does not address malicious links inside Unified Communications products.	–
Link Clickthrough Protections 3.PEP.UN.LCTPR	–	–	Cloudflare does not address link click-through inside Unified Communications products.	
Malicious File Protections 3.PEP.UN.MFPRO	–	–	Cloudflare does not address malicious files found inside Unified Communications products.	

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Data Protection (DA) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Access Control 3.PEP.DA.ACONT	✅ Cloudflare Access Cloudflare Gateway	–	Cloudflare SASE/SSE provides a suite of access controls that can be applied towards applications and resources onboarded to Cloudflare Access and traffic that passes through Cloudflare's edge (via Gateway)	Reference architecture
Protections for Data at Rest 3.PEP.DA.PDRES	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare Cloud Access Security Broker (CASB)	–	Cloudflare's API CASB can identify data at rest in SaaS applications that matches DLP profiles and has an inappropriate level of access or exposure	Reference architecture
Protections for Data in Transit 3.PEP.DA.PDTRA	✅ Cloudflare Gateway Cloudflare Access Cloudflare TLS/SSL	–	Cloudflare's DLP profiles can protect data in motion when applied to the appropriate Gateway policy. Cloudflare SSL/TLS allows websites and applications to establish secure connections. Cloudflare can provide edge, client, and origin certificates with different configurations possible.	Reference architecture
Data Loss Prevention 3.PEP.DA.DLPRE	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare Gateway Cloudflare API Gateway Cloudflare Cloud Access Security Broker (CASB)	–	Cloudflare DLP profiles matched within SaaS applications onboarded to Cloudflare's API CASB or within Gateway-filtered traffic will be flagged inside CASB findings or gateway logs, respectively. In context of self-hosted applications, sensitive data detection and API Gateway alerts on webapps or API responses containing sensitive data.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Data Protection (DA) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Data Access and Use Telemetry 3.PEP.DA.DAUTE	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare Gateway Cloudflare Cloud Access Security Broker (CASB)	–	Cloudflare's API CASB can identify sensitive data stored in SaaS applications with an inappropriate level of exposure or access (by matching it against DLP profiles). Cloudflare's Gateway policies that include DLP profiles can identify where and when sensitive information transmission was attempted and blocked.	Reference architecture Cloudflare Logs
Data Labeling 3.PEP.DA.DLABE	–	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare Cloud Access Security Broker (CASB)	Cloudflare DLP integration profiles can identify data based on information type (financial, medical, code, etc.), or based on any regex criteria specified by the user. Integration profiles enable data loss prevention support for third-party data classification providers. Data classification information is retrieved from the third-party platform and populated into a DLP Profile. You can then enable detection entries in the profile and create a DLP policy to allow or block matching data. Detection entries in integration profiles are managed by the third-party platform and cannot be manually added, edited, or deleted within Cloudflare DLP. **Important**: Integration profiles require Cloudflare CASB.	Data loss protection Integration profiles Cloud Access Security Broker
Data Inventory 3.PEP.DA.DINVE	–	✅ Cloudflare R2 Cloudflare Workers	Cloudflare offers data inventory and storage for a range of use cases. For example, Cloudflare R2 helps you manage storage for cloud-native applications, web content, podcast episodes, data lakes (analytics and big data), and large batch processes such as machine learning model artifacts or datasets, And Cloudflare Workers supports a range of storage and database options for key-value stores (Cloudflare Workers KV) through to SQL databases (Cloudflare D1). **Important**: Cloudflare is not an Enterprise Data Inventory (EDI) or Data Management Platform (DMP)	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Services (SE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Active Content Mitigation 3.PEP.SE.ACMIT	✅ Cloudflare Browser Isolation	✅ Cloudflare Page Shield	Cloudflare Browser Isolation complements the Secure Web Gateway and Zero Trust Network Access solutions by executing active webpage content in a secure isolated browser. Executing active content remotely from the endpoint protects users from zero-day attacks and malware. In addition to protecting endpoints, Browser Isolation also protects users from phishing attacks by preventing user input on risky websites and controlling data transmission to sensitive web applications. You can further filter isolated traffic with Gateway HTTP and DNS policies. Cloudflare Page Shield helps defend against client-side attacks, It protects websites' end users from client-side attacks that target vulnerable JavaScript dependencies in order to run malicious code in the victim's browser. **Important**: Cloudflare Page Shield is not FedRAMP authorized at this time.	Reference architecture
Data Loss Prevention 3.PEP.SE.DLPRE	✅ Cloudflare Data Loss Prevention (DLP) Cloudflare API Gateway	–	Cloudflare Data Loss Prevention (DLP) can help prevent data exfiltration by detecting and stopping files while in-transit, based on sensitive data-matching DLP profiles. In context of self-hosted applications, sensitive data detection and API Gateway alerts on webapps or API responses containing sensitive data.	Cloudflare Data Loss Prevention
Protocol Compliance Enforcement 3.PEP.SE.PCENF	✅ Cloudflare Gateway Cloudflare Magic Firewall Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway networking rules and Cloudflare Magic Firewall rules can be used to enforce the use of specific protocols and ports against L3 destinations. WAF allows customers to enable rules to block requests based on many different HTTP attributes and protocol violations like invalid HTTP Request Line or Content-Length HTTP header issues.	Reference architecture
Malicious Content Filtering 3.PEP.SE.MCFIL	✅ Cloudflare Gateway Cloudflare Web Application Firewall (WAF)	–	Cloudflare Gateway enables users to detect malicious content and prevent users from navigating to sites classified as security threats or downloading malicious files, respectively. Cloudflare WAF's Uploaded Content Scanning can detect and block malicious file uploads, applicable only to files in plain text in the response body.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Services (SE) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Access Control 3.PEP.SE.ACONT	✅ Cloudflare Gateway Cloudflare API Gateway Cloudflare Browser Isolation	–	Cloudflare RBI policies can require websites rendered in an isolated browser. These remote browsers contain data protection controls that can limit user activities like copy/paste, uploads/downloads, and keyboard usage. Gateway Network policies can define which ports and protocols can be used to communicate with L3 destinations, which would include machine-to-machine communication or 'entities' Gateway HTTP policies can be used to prevent HTTP methods from being executed on a specific webpage, for example preventing users from deleting items via HTTP DELETE method. These policies can include identity-based and posture-based access controls as a criteria of execution. Cloudflare API Gateway allows users to upload an API schema restricting what endpoints can be called and how they can be used.	Reference architecture

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Identity (ID) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Adaptive Authentication 3.PEP.ID.AAUTH	–	✅ Cloudflare Access	Cloudflare Access determines who can reach your application by applying the Access policies you configure. An Access policy consists of an Action as well as rules which determine the scope of the action. Cloudflare's user risk scoring employs AI/machine learning techniques to analyze the real-time telemetry of user activities and behaviors that pass through our network. It helps identify abnormal behavior and potential indicators of compromises that could lead to danger for your organization, so your security teams can lock down suspicious activity and adapt your security posture in the face of changing risk factors and sophisticated threats	Cloudflare Access policies Cloudflare user risk scoring
Service Identity 3.PEP.ID.SIDEN	–	✅ Cloudflare API Gateway	Cloudflare API Gateway authenticates the identity of agency services through SSL/TLS certificates. It supports Mutual TLS (mTLS) authentication using client certificates to ensure traffic between client and server is bidirectionally secure and trusted. mTLS also allows requests that do not authenticate via an identity provider, such as Internet-of-things (IoT) devices, to demonstrate they can reach a given resource. API Gateway's JWT Validation stops JWT replay attacks and JWT tampering by cryptographically verifying incoming JWTs before they are passed to the API origin. JWT Validation will also stop requests with expired tokens or tokens that are not yet valid.	Cloudflare API Gateway certificates
Entitlement Inventory 3.PEP.ID.EINVE	–	✅ Cloudflare Access	Cloudflare maintains an inventory of user and entity access rights for specific resources (which have been onboarded to Cloudflare).	Cloudflare App Launcher Cloudflare WARP
Secrets Management 3.PEP.ID.SMANA	✅ Cloudflare Secrets Store	✅ Cloudflare API Gateway Cloudflare Web Application Firewall (WAF)	Cloudflare Secrets Store enables developers to securely store and manage application secrets like API tokens and authorization headers. Cloudflare allows for creating and managing mTLS certificates which can be used with sites and by API Gateway/WAF for mTLS authentication for API endpoints. Additionally, API Gateway allows for JWT validation upon API endpoint requests. Cloudflare One has a 'Service Authentication' tool that allows users to generate tokens, mTLS certs, and short lived certificates that can be used to authenticate employees or entities to specific resources.	Cloudflare Secrets

Cloudflare Service(s) - Detailed Mapping

Policy Enforcement Point (PEP) Security Capabilities

Identity (ID) Capability Group

TIC Security Capability	Primary Service(s)	Complementary Service(s)	Service Description	Configuration Guidance
Behavioral Baselining 3.PEP.ID.BBASE	–	✅ Cloudflare Secure Access Service Edge (SASE) Cloudflare Bot Management Cloudflare API Gateway Cloudflare Web Application Firewall (WAF)	Cloudflare Zero Trust solutions can evaluate user risk in the context of prohibited activities (such as impossible travel or number of DLP policies triggered), but by default does not create unique baselines of individual user behavior. Cloudflare keeps a baseline of traffic volume and patterns across sites to detect for anomalies around activity and performance and any potentially malicious behavior. Bot Mgmt builds a baseline for detecting anomalies. API Gateway builds a baseline to provide recommendations on rate limiting per endpoint to protect against abuse. WAF uses machine learning to detect variations designed to bypass WAF and uses this data to enhance the machine learning models used.	Cloudflare Zero Trust
Enterprise Identity and Access Management 3.PEP.ID.EIAMA	–	✅ Cloudflare Access	Cloudflare integrates with enterprise Identity Providers (IdP) for user provisioning, and Cloudflare Access supports the System for Cross-domain Identity Management (SCIM) for all SAML and OIDC identity providers that use SCIM version 2.0. This enables you to synchronize user identity information across cloud applications and services. Cloudflare can help manage changes to access rights, but does not change the user identities themselves. Cloudflare also supports a wide range of Multi-Factor Authentication (MFA), and provides Single Sign-On across applications. **Important**: Cloudflare is not an Identity Provider (IdP), and does not provide enterprise-wide Identity Credential and Access Management (ICAM) capabilities for other products or technologies. Cloudflare integrates with leading IdPs like Okta and Microsoft.	Cloudflare Access Cloudflare Access for SaaS Cloudflare App Launcher Cloudflare SCIM Provisioning
Multi-factor Authentication 3.PEP.ID.MAUTH	–	✅ Cloudflare Access	Cloudflare Access can require that users log in to certain applications with specific types of multifactor authentication (MFA) methods. For example, you can create rules that only allow users to reach a given application if they authenticate with a physical hard key.	Enforce MFA
Continuous Authentication 3.PEP.ID.CAUTH	–	✅ Cloudflare Access Cloudflare Gateway	Cloudflare Access enables administrators to set session durations for every onboarded application, requiring users to reauthenticate if they leave the session and return after a certain amount of time. Cloudflare's 'WARP Client Session duration' feature means users will need to re-authenticate if their session lasts beyond a certain duration.	Cloudflare WARP Cloudflare WARP sessions

Let Cloudflare help you accomplish your TIC 3.0 goals

Every public sector organization is under pressure to modernize cyber security architectures, deliver trustworthy digital services, eliminate technology debt, and comply with multiple regulatory mandates. At Cloudflare, we're your trusted partner to help you accomplish all of your top priorities.

Protect

Mitigate risk with advanced security capabilities

- Mature Zero Trust architectures
- Deliver resilient public-facing applications
- Detect and respond proactively

Connect

Power everything with an intelligent connectivity cloud

- Work and learn from anywhere
- Optimize network and app performance
- Enhance service resilience

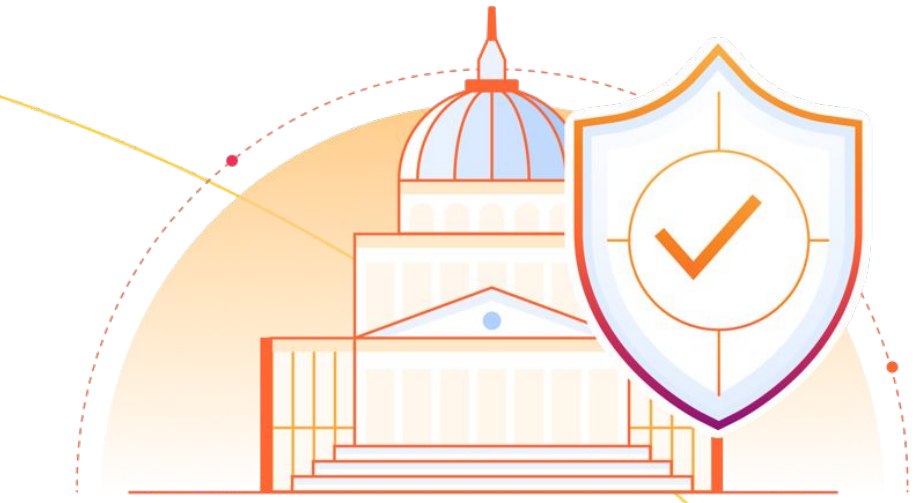
Accelerate

Modernize faster and increase operational efficiency

- Eradicate legacy technology
- Reduce costs and complexity
- Achieve continuous compliance

Are you ready to protect, connect, and accelerate your public sector mission?

Learn more about Cloudflare for Public Sector, or contact us today.



1 888 99 FLARE | cloudflare.com/public-sector

© 2025 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

REV:PMM-FEB2025