CLOUDFLARE

WHITE PAPER

Advancing data protection and compliance in Higher Education

Cloudflare aligns with NIST guidance
for continuous compliance

Protecting CUI is mandatory

From student aid information to federal research data, higher education institutions hold a sensitive category of government data called Controlled Unclassified Information (CUI). The National Archives defines CUI as "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies."

The Gramm Leach Bliley Act (GLBA) is one such applicable law, requiring extensive security and privacy controls to protect student financial records and personally identifiable information. Another is the Cybersecurity Maturity Model Certification (CMMC), to protect government research data and intellectual property. Non-compliance can lead to severe consequences, including the loss of existing federal funding, ineligibility for future research opportunities, and significant financial and reputational damage stemming from data breaches.

NIST guidance for CUI protection

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," defines the security requirements for protecting Controlled Unclassified Information (CUI) when it resides outside of the government's direct control.

Therefore, NIST SP 800-171 is critical guidance for higher education institutions required to secure student aid data under GLBA, covered defense information under CMMC, student records under FERPA, health information under HIPAA, and research data from industry partnerships.

Did you know?

Major university settles cyber non-compliance for $1.25M

In 2024, a major research university paid the US government $1.25 million to settle CMMC compliance violations, including the failure to use a FedRAMP authorized cloud services provider for some government contracts.

Cloudflare helps protect CUI and accelerates compliance

As a FedRAMP® authorized cloud services provider for the federal government, Cloudflare has the essential security capabilities to satisfy many NIST SP 800-171 requirements. This paper maps our capabilities directly to them to clarify where we can help.

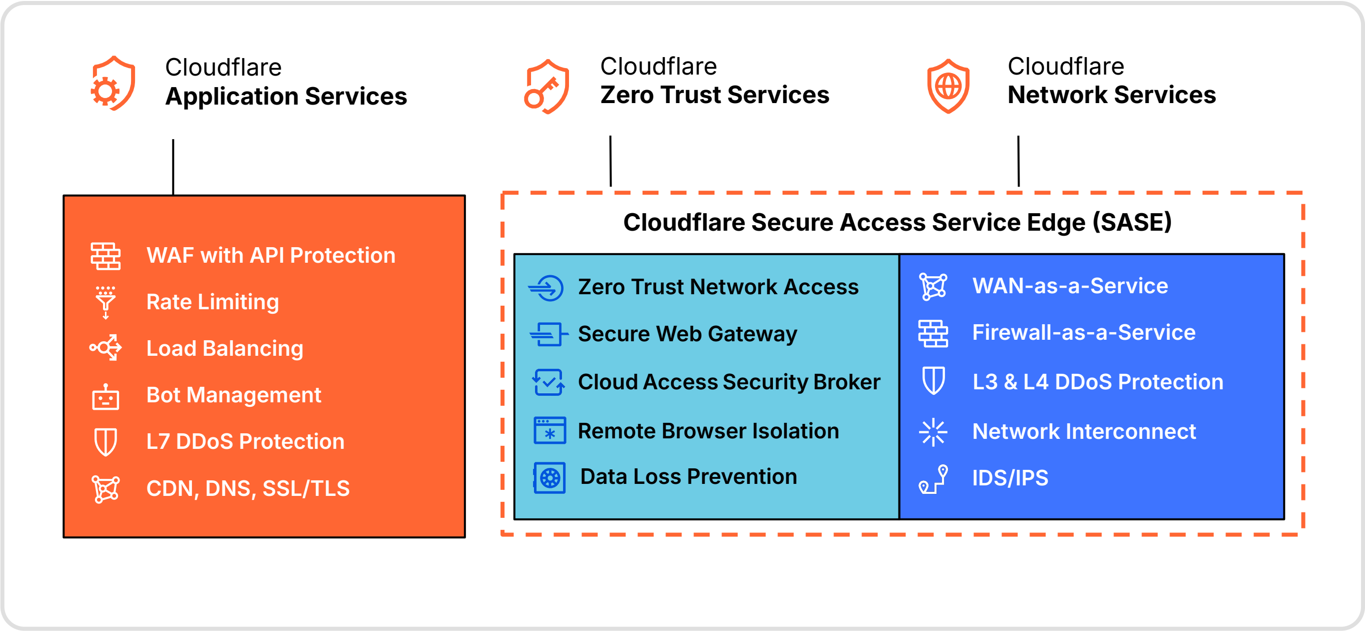
In Table 1, the green check marks represent our primary mappings at the control family level, and the following pages provide detailed Cloudflare capability mappings against the full set of NIST requirements.

Table 1: NIST SP 800-171 Security Requirement Families

✅ Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	✅ System and Comms Protection
✅ Audit and Accountability	Personnel Security	✅ System and Information Integrity
Configuration Management	Physical Protection	Planning
✅ Identification and Authentication	Risk Assessment	System and Services Acquisition
✅Incident Response		Supply Chain Risk Management

Cloudflare services that support NIST SP 800-171 requirements

Cloudflare's modern application services, Zero Trust solutions, and network services help organizations efficiently and effectively comply with regulatory requirements. While our platform includes a vast portfolio of individual solutions, the diagram below highlights the most relevant solution areas.



Cloudflare **Application Services**

- WAF with API Protection
- Rate Limiting
- Load Balancing
- Bot Management
- L7 DDoS Protection
- CDN, DNS, SSL/TLS

Cloudflare **Zero Trust Services**

Cloudflare **Network Services**

Cloudflare Secure Access Service Edge (SASE)

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker
- Remote Browser Isolation
- Data Loss Prevention

- WAN-as-a-Service
- Firewall-as-a-Service
- L3 & L4 DDoS Protection
- Network Interconnect
- IDS/IPS

Cloudflare Application Services

Security and performance for web applications

Stop bad bots, protect applications and APIs from abuse, and thwart DDoS attacks, all powered by built-in threat intelligence gathered from the Cloudflare connectivity cloud, which blocks an average of ~247 billion threats per day.

Increase web application performance with infinitely scalable connectivity across over 330 global cities.

Cloudflare Zero Trust Services

Simplify SSE & SASE adoption

Modernize your network and protect your workforce with our unified cloud-native platform

Too many SSE and SASE journeys are held back by disjointed 'platforms' saddled with tech debt. Cloudflare's connectivity cloud is the modern answer — a composable, cloud-native platform that adapts to any use case.

Cloudflare Network Services

Modernize your network infrastructure

Eliminate networking and security appliances, and adopt the Cloudflare connectivity cloud. It delivers secure, fast, and reliable service to any point in the world, and easily adapts to new business requirements.

Strengthen your business continuity, improve the user experience, and reduce operating costs

3.1 - Access Control

Identifier	Description	Cloudflare services
03.01.01	Account management	- 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. - **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, but integrates with leading IdPs like Okta and Microsoft through the Cloudflare Technology Partners program.
03.01.02	Access Enforcement	- 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.
03.01.03	Information Flow Enforcement	- Cloudflare Regional Services, part of our Data Localization Suite, helps you enforce where your data is handled, without losing the security and performance benefits our network provides. The Customer Metadata Boundary ensure that data containing sensitive information does not leave the region you specify.
03.01.04	Separation of Duties	- Cloudflare Access determines who can reach your application by applying the separation of duties policies you configure.
03.01.05 **03.01.06** **03.01.07**	Least Privilege (for end users, privileged accounts, and functions)	- Cloudflare Access enforces least privilege by enabling granular access policies so that users can access only the resources needed to perform their job functions.
03.01.08	Unsuccessful Logon Attempts	- Cloudflare integrates with enterprise Identity Providers (IdP) that enforce unsuccessful logon policies, preventing users who fail to authenticates after multiple attempts from reaching critical resources.
03.01.09	System Use Notification	- Cloudflare integrates with enterprise Identity Providers (IdP) that can place system use notification warnings and banners on their login widgets.
03.01.10	Device Lock	- Cloudflare does not provide device locks that are typically implemented at the operating system level or the application level.
03.01.11	Session Termination	- Cloudflare Access performs continuous identity evaluation, a Zero Trust security model that eliminates the need for most of the user-interrupting workflows triggered by session timeouts, but you can still configure session timeouts.
03.01.12	Remote Access	- Cloudflare Access secures remote access through Zero Trust Network Access (ZTNA) that verifies context (like identity and device posture) to secure access across your entire environment — no VPN required.
03.01.16	Wireless Access	- Cloudflare does not provide wireless access.
03.01.19	Access Control for Mobile Devices	- Cloudflare Mobile Device Management partnerships help secure endpoints for your remote workforce by deploying Cloudflare's client with mobile device management (MDM) vendors of your choice.
03.01.20	Use of External Systems	- Cloudflare Access restricts access to external applications according to your security policy.
03.01.22	Publicly Accessible Content	- Process-related control

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

3.2 - Awareness and Training

Identifier	Description	Cloudflare services
03.02.01	Literacy Training and Awareness	- While Cloudflare does not provide general-purpose cyber education, the Cloudflare Learning Center provides resources on cyber security and how the Internet works.
03.02.02	Role-Based Training	- For specialized roles responsible for Cloudflare solutions, Cloudflare Docs provides important resources, guides and tutorials to learn how to architect, deploy, integrate and use Cloudflare technology.

3.3 - Audit and Accountability

Identifier	Description	Cloudflare services
03.03.01	Event Logging	- Process-related control
03.03.02	Audit Record Content	- Cloudflare Logs are detailed logs that contain metadata generated by our products, helpful for debugging, identifying configuration adjustments, and creating analytics, especially when combined with logs from other sources, such as your application server.
03.03.03	Audit Record Generation	- 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, but integrates with leading logging and analytics solutions through Cloudflare's Technology Partnership Program.
03.03.04	Response to Audit Logging Process Failures	- Process-related control
03.03.05	Audit Record Review, Analysis, and Reporting	- Cloudflare Log Explorer enables you to store and explore your Cloudflare logs directly within the Cloudflare Dashboard or API. Giving you visibility into your logs without the need to forward them to third parties. Logs are stored on Cloudflare's global network using the R2 object storage platform and can be queried via the Dashboard or SQL API.
03.03.06	Audit Record Reduction and Report Generation	- Cloudflare Analytics visualizes the metadata collected by our products in the Cloudflare dashboard that supports audit record review, analysis, reporting requirements, and after-the-fact incident investigation.
03.03.07	Time Stamps	- Cloudflare Time Services generate time stamps for Cloudflare Logs and audit records. Cloudflare Time Services also supports Network Time Security (NTS) to maintain the integrity of all time stamps.
03.03.08	Protection of Audit Information	- Cloudflare logs are stored on Cloudflare R2 object storage that protects audit information with encryption both in transit and at rest.

3.4 - Configuration Management

Identifier	Description	Cloudflare services
03.04.01	Baseline Configuration	- Process-related control
03.04.02	Configuration Settings	- 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.
03.04.03	Configuration Change Control	- Cloudflare Version Management enables you to safely test, deploy, and roll back changes to your zone configurations in a staging environment. - **Important**: Cloudflare does not offer an Enterprise Configuration Management (ECM) solution.
03.04.04	Impact Analyses	- Process-related control
03.04.05	Access Restrictions for Change	- Cloudflare roles and scope help ensure that only authorized individuals are able to make configuration changes.
03.04.06	Least Functionality	- Cloudflare enables you to configure and deploy only mission-essential capabilities, helping to implement the principle of least functionality.
03.04.08	Authorized Software – Allow by Exception	- Process-related control
03.04.10	System Component Inventory	- 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.
03.04.11	Information Location	- Process-related control
03.04.12	System and Component Configuration for High-Risk Areas	- Cloudflare does not address discrete systems or system component that customers move to high-risk physical locations.

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

Solution spotlight

Cloudflare Security Center

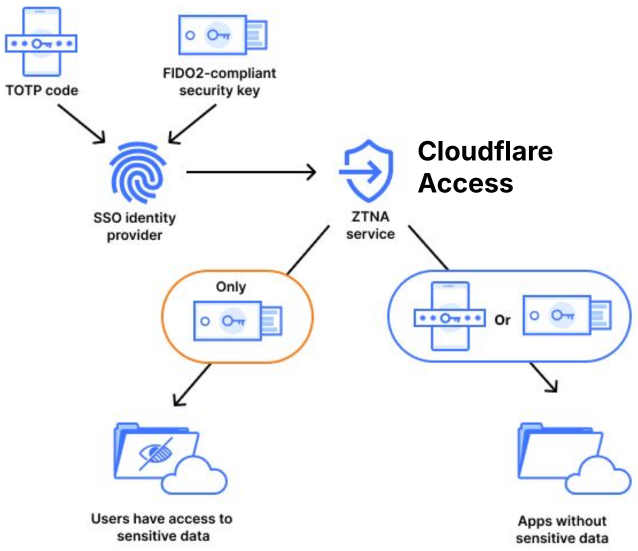
Cloudflare Security Center brings together our suite of security products, our security expertise, and our unique Internet intelligence as a unified security intelligence solution.

- Identify unknown assets
- Detect rogue assets
- Identify third-party risks

3.5 - Identification and Authentication

Identifier	Description	Cloudflare services
03.05.01	User Identification and Authentication	- Cloudflare integrates with enterprise Identity Providers (IdP) that uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.
03.05.02	Device Identification and Authentication	- Cloudflare Zero Trust can use device serial numbers or device UUIDs (via MDM integration) to grant access to users with authorized devices before establishing system connections.
03.05.03	Multi-Factor Authentication	- Cloudflare Zero Trust policies 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. - **Important**: MFA requires integration with an identity provider (IdP) integration via Okta, Microsoft Entra ID (formerly Azure AD), OpenID Connect (OIDC), or the Security Assertion Markup Language (SAML)
03.05.04	Replay-Resistant Authentication	- Cloudflare Zero Trust can enforce FIDO2 MFA (replay-resistant or phishing-resistant MFA) consistently across SaaS, self-hosted, and non-web resources.
03.05.05	Identifier Management	- Process-related control
03.05.07	Password Management	- Cloudflare integrates with enterprise Identity Providers (IdP) that manage end users passwords.
03.05.11	Authentication Feedback	- Cloudflare integrates with enterprise Identity Providers (IdP) that control authenticator feedback through their sign-on widgets.
03.05.12	Authenticator Management	- Process-related control

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.


TOTP code
FIDO2-compliant security key
SSO identity provider
Cloudflare Access
ZTNA service
Only
Or
Users have access to sensitive data
Apps without sensitive data

How it works

Defeat phishing with FIDO2 MFA and Cloudflare

Cloudflare's Zero Trust platform can enforce Fast IDentity Online 2 (FIDO2) MFA consistently across SaaS, self-hosted, and non-web resources.

1. Implement Cloudflare Access, our Zero Trust Network Access (ZTNA) service.
2. Bolster security with FIDO2-compliant, replay-resistant MFA.
3. Enforce replay-resistant MFA for all sensitive apps.

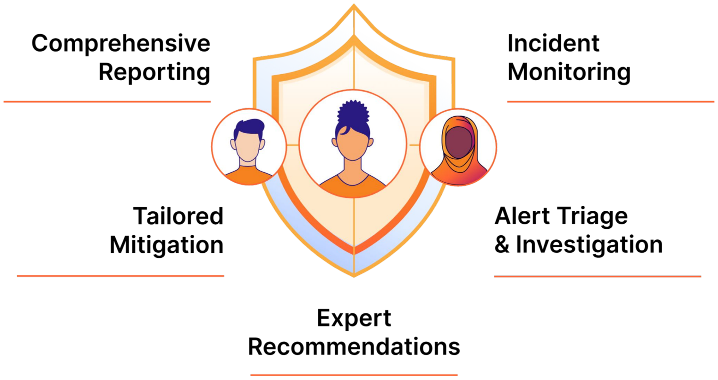
3.6 - Incident Response

Identifier	Description	Cloudflare services
03.06.01	Incident Handling	• While this is a process-related control, Cloudflare SOC-as-a-Service can help your team with preparation, detection and analysis, containment, eradication, and recovery.
03.06.02	Incident Monitoring, Reporting, and Response Assistance	• While this is a process-related control, the Cloudflare SOC-as-a-Service team follows programmatic threat monitoring and response process for consistency across incident triage, investigation, and remediation.
03.06.03	Incident Response Testing	• Process-related control
03.06.04	Incident Response Training	• Process-related control
03.06.05	Incident Response Plan	• While this is a process-related control, Cloudflare SOC-as-a-Service helps you follow incident response plans through alert triage, investigation, expert recommendations, tailored mitigation, and comprehensive reporting.

Let Cloudflare improve your incident detection and response capabilities

With Cloudflare security operations center-as-a-service, our dedicated team of Cloudflare security operations engineers will monitor your environment for security threats and potential operational disruptions; perform deep analysis to identify attack vectors, and help you implement countermeasures to mitigate future incidents.

It's designed to meet the network and application security monitoring, threat detection and incident response needs of enterprises of all sizes and sophistication.



Solution spotlight

Cloudflare SOC-as-a-Service

Cloudflare SOC team follows programmatic threat monitoring and response process - bringing immediate consistency across incident triage, investigation, and remediation

- Global, 24/7/365 protection
- < 30 mins security incident response SLA
- SOC support available for core and network

3.7 - Maintenance

Identifier	Description	Cloudflare services
03.07.04	Maintenance Tools	- Process-related control
03.07.05	Nonlocal Maintenance	- Process-related control
03.07.06	Maintenance Personnel	- People and process-related control

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

3.8 - Media Protection

Identifier	Description	Cloudflare services
03.08.01	Media Storage	- Cloudflare does not address media protection
03.08.02	Media Access	- Cloudflare does not address media protection
03.08.03	Media Sanitization	- Cloudflare does not address media protection
03.08.04	Media Marking	- Cloudflare does not address media protection
03.08.05	Media Transport	- Cloudflare does not address media protection
03.08.07	Media Use	- Cloudflare does not address media protection
03.08.09	System Backup – Cryptographic Protection	- Cloudflare does not address media protection

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

3.9 - Personnel Security

Identifier	Description	Cloudflare services
03.09.01	Personnel Screening	- Cloudflare does not screen personnel
03.09.02	Personnel Termination and Transfer	- Cloudflare supports the System for Cross-domain Identity Management (SCIM) to synchronize identity information and adjust access rights for transfer/termination.

3.10 - Physical Protection

Identifier	Description	Cloudflare services
03.10.01	Physical Access Authorizations	- Cloudflare does not address physical protection
03.10.02	Monitoring Physical Access	- Cloudflare does not address physical protection
03.10.06	Alternate Work Site	- Cloudflare does not address physical protection
03.10.07	Physical Access Control	- Cloudflare does not address physical protection
03.10.08	Access Control for Transmission	- Cloudflare does not address physical protection

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

3.11 - Risk Assessment

Identifier	Description	Cloudflare services
03.11.01	Risk Assessment	- Process-related control
03.11.02	Vulnerability Monitoring and Scanning	- Cloudflare Security Center scans known assets, identifies unknown assets, and detect rouge assets to map the attack surface and identify potential vulnerabilities. - Cloudflare WAF offers Cloudflare Managed Rules, OWASP Core Ruleset, and Exposed Credential Check to help defend against new vulnerabilities and reduce false positives. - **Important**: Cloudflare is not an Enterprise Vulnerability Management solution.
03.11.04	Risk Response	- Process-related control

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

> "With the Cloudflare platform, we're getting very high-powered, very technical [application security] detection and protections that take little to no effort to deploy — that's especially important for our organizations that already struggle with limited resources."

Deputy Director and Interim State CISO
State of Arizona

3.12 - Security Assessment and Monitoring

Identifier	Description	Cloudflare services
03.12.01	Security Assessment	- Process-related control
03.12.02	Plan of Action and Milestones	- Process-related control
03.12.03	Continuous Monitoring	- Process-related control
03.12.05	Information Exchange	- Process-related control
03.12.08	Access Control for Transmission	- Process-related control

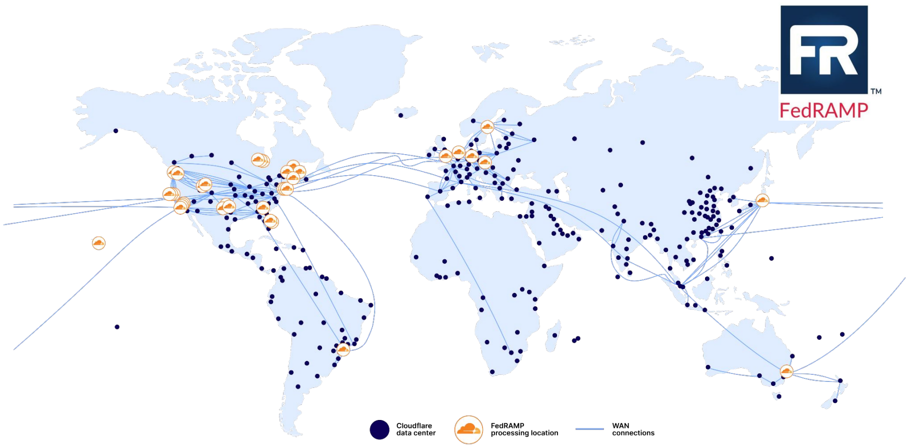
Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

The Cloudflare global network

FedRAMP® Moderate Authorized and committed to High

Our vast global network, which is one of the fastest on the planet, is trusted by millions of web properties.

With direct connections to nearly every service provider and cloud provider, the Cloudflare network can reach about 95% of the world's population within approximately 50 ms.



Innovation everywhere

Our single-platform approach ensures every innovation is available in every data center, including our FedRAMP processing locations

Continuous investment

We're expanding our FedRAMP processing locations both within the US and internationally to strengthen security and performance around the globe

Agility always

We're deploying tomorrow's requirements today, like post-quantum cryptography, to secure your mission today – and tomorrow

3.13 - System and Communication Protection

Identifier	Description	Cloudflare services
03.13.01	Boundary Protection	• Cloudflare Access is our Zero Trust Network Access (ZTNA) solution that protects the boundary between the public Internet and internal applications by ensuring only authorized individuals with authorized, secure devices can access them. • Cloudflare Gateway is our Secure Web Gateway (SWG) that protects the boundary between your internal users and the public Internet by stopping threats like ransomware, phishing, and malware command and control. It controls and monitors transport layer (L4) to application layer (L7) traffic with DNS, HTTP, network, and browser isolation rules, while enforcing acceptable use policies. • Cloudflare Web Application Firewall (WAF) secures the boundary between the public Internet and your public-facing applications using threat intelligence and machine learning powered by platform intelligence from the Cloudflare connectivity cloud to stop application threats, including zero-day exploits. • Cloudflare DNS secures the boundary between the public Internet and your Domain Name System (DNS) infrastructure to maintain its integrity. For example, it enables you to configure email security DNS records to stop phishers from sending emails from your domain. • Cloudflare DDoS Protection secures the boundary between the public Internet and your users, applications, and infrastructure by stopping distributed denial-of-service (DDoS) attacks from reaching them, ensuring uptime and service resilience. • Cloudflare Email Security secures the boundary between the public Internet and your users email inboxes by blocking and isolating phishing threats, including email-borne malware, business email compromise (BEC), and multi-channel (link-based) attacks. • Cloudflare Browser Isolation is our Remote Browser Isolation (RBI) solution that protects the boundary between the public Internet and devices by running code at the edge of our global network — preventing threats like ransomware, phishing, and zero-day browser vulnerabilities from reaching users' devices. • Cloudflare Data Loss Protection is our Data Loss Protection (DLP) solution that secures the boundary between your internal endpoints (devices) and the public Internet by detecting and preventing data exfiltration, data destruction, leakage and loss of confidential information. • Cloudflare Magic Firewall is our cloud-based firewall (firewall-as-a-service) that secures the boundary between the public Internet and internal systems by filtering network traffic based on protocol, port, IP addresses, consistently enforce security policies globally without the overhead of managing on-premises appliances. • Cloudflare CASB is our Cloud Access Security Broker (CASB) that secures the boundary between user devices and SaaS applications by preventing users from submitting sensitive data into unauthorized SaaS apps. It stops "shadow IT," or the use unsanctioned SaaS applications, and detects and remediate misconfigurations that risk data exposure and code leaks. • Cloudflare Tunnel protects the boundary between your internal applications and the public Internet by securely connecting them to Cloudflare's network without a publicly routable IP address, enabling secure clientless access. You send no traffic to an external IP; instead, a lightweight daemon in your infrastructure (cloudflared) creates outbound-only connections to Cloudflare's global network so your origins can serve traffic through Cloudflare without being vulnerable to attacks that bypass Cloudflare.

"We were able to add layers to our security defenses with Cloudflare. The more layers you add, the more difficult it is for attackers to succeed in making voters question the trust of the democratic process that we work to protect every day."

Stacy Mahaney, Chief Information Officer
State of Missouri

3.13 - System and Communication Protection

Identifier	Description	Cloudflare services
03.13.05	Information in Shared System Resources	- Cloudflare CASB is our Cloud Access Security Broker (CASB) that prevents users from submitting sensitive data into unsanctioned SaaS apps that can lead to unauthorized and unintended information transfer from these shared resources. - Cloudflare Data Loss Protection is our Data Loss Protection (DLP) solution that prevents unauthorized and unintended information transfer by detecting and preventing data exfiltration and leakage.
03.13.06	Network Communications – Deny by Default – Allow by Exception	- Cloudflare Magic Firewall is our cloud-based firewall (firewall-as-a-service) that controls network communications, denies by default, and allows by exception by filtering network traffic based on protocol, port, IP addresses, consistently enforce security policies globally without the overhead of managing on-premises appliances.
03.13.08	Transmission and Storage Confidentiality	- Cloudflare Magic WAN is our cloud-delivered enterprise networking solution that provides encrypted any-to-any network connectivity across campuses, branches and data centers. - Cloudflare Post-Quantum Cryptography (PQC) defends against "harvest now, decrypt later" attacks through our PQC implementation that employs the FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standard - Cloudflare R2 object storage encrypts data in transit and at rest.
03.13.09	Network Disconnect	- This is an operating system level and application level control.
03.13.10	Cryptographic Key Establishment and Management	- Cloudflare SSL/TLS Certificates ensure that data passing between users and servers is encrypted.
03.13.11	Cryptographic Protection	- Cloudflare SSL/TLS Certificates ensure that data passing between users and servers is encrypted. - Cloudflare Post-Quantum Cryptography (PQC) defends against "harvest now, decrypt later" attacks through our PQC implementation that employs the FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standard
03.13.12	Collaborative Computing Devices and Applications	- Cloudflare Access ensures that only authorized devices can reach approved applications.
03.13.13	Mobile Code	- Cloudflare Page Shield simplifies third-party script management by tracking loading resources (like scripts) for potentially malicious additions, connections, or changes. - Cloudflare Web Application Firewall (WAF) scans uploaded code for malware in uploaded files.
03.13.15	Session Authenticity	- Cloudflare Web Application Firewall (WAF) defends against adversary-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

Important: The identifiers in this list are not sequential because NIST either withdrew controls or incorporated them into other controls.

"Even though the transition to **post-quantum cryptography** is starting before a cryptographically relevant quantum computer has been built, there is a pressing threat. Encrypted data remains at risk because of the "harvest now, decrypt later" threat in which adversaries collect encrypted data now with the goal of decrypting it once quantum technology matures" (NIST IR 8547)

NIST

3.14 - System and Information Integrity

Identifier	Description	Cloudflare services
03.14.01	Flaw Remediation	• Cloudflare Security Center scans known assets, identifies unknown assets, and detect rouge assets to map the attack surface and identify potential vulnerabilities, and recommends mitigation actions. • **Important**: Cloudflare is not an Enterprise Vulnerability Management solution.
03.14.02	Malicious Code Protection	• Cloudflare Email Security protects against malware that arrives by email. • Cloudflare Web Application Firewall (WAF) provides malicious uploads detection, also called uploaded content scanning, to prevent malicious content from infecting your web applications. • Cloudflare Zero Trust services can restrict access to sensitive resources based on the device posture signals from our partners' endpoint security platforms, preventing malware and malicious code present compromised devices from reaching and infecting internal applications. • **Important**: Cloudflare is not an Endpoint Detection and Response (EDR) solution.
03.14.03	Security Alerts, Advisories, and Directives	• Process-related control
03.14.06	System Monitoring	• The Cloudflare Global Network – our connectivity cloud – is our unique platform for external and internal system monitoring, detection, and response. Since our platform is global, we can monitor at strategic locations including your perimeter locations, near server farms that support critical applications, at peering points with other Internet service providers – essentially everywhere. • Cloudforce One is our security intelligence and operations solution that makes 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. • Cloudflare Security Center monitors your internal environment and the external Internet, maps your attack surface and identifies potential vulnerabilities – improving security with threat intelligence data from Cloudflare's massive global network which protects about 20% of all websites.
03.14.08	Information Management and Retention	• Process-related control

Cloudflare differentiator

Cloudforce One

Our world-class threat research combines visibility into real-time attack traffic with a world-class threat research team for unmatched operational threat intelligence.

- Actionable threat intelligence
- Faster, more in-depth investigations
- Disrupt attacks with sinkholing

3.15 - Planning

Identifier	Description	Cloudflare services
03.15.01	Policy and Procedures	- Process-related control
03.15.02	System Security Plan	- Process-related control
03.15.03	Rules of Behavior	- Process-related control

3.16 - System and Services Acquisition

Identifier	Description	Cloudflare services
03.16.01	Security Engineering Principles	- Process-related control
03.16.02	Unsupported System Components	- Process-related control
03.16.03	External System Services	- As a FedRAMP-authorized cloud services provider, Cloudflare meets security requirements established by the Government for the FedRAMP Moderate baseline as required under DFARS 252.204-7012.

3.17 - Supply Chain Risk Management

Identifier	Description	Cloudflare services
03.17.01	Supply Chain Risk Management Plan	- Process-related control
03.17.02	Acquisition Strategies, Tools, and Methods	- Process-related control
03.17.03	Supply Chain Requirements and Processes	- As a FedRAMP-authorized cloud services provider, Cloudflare is committed to being a trusted partner and a key part of your security, application, and network supply chain.

NIST SP 800-171 taught us a lot about protecting sensitive information.

But NIST also has great guidance on supply chain security too. Check out NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, which provides critical steps to manage cyber supply chain risks throughout your organization.

NIST

Accomplish all of your priorities with speed, simplicity, and confidence

By partnering with Cloudflare, we can help you accomplish your goals and build trust in the future of education.

Protect

Secure data and protect privacy with modern cyber security

- Enhance institutional resilience
- Stop disruptive cyber attacks
- Achieve continuous compliance

Connect

Enhance digital service performance and resilience

- Deliver trustworthy digital services
- Integrate into existing ecosystems
- Optimize networks and data centers

Accelerate

Modernize faster and boost operational efficiency

- Innovate faster with the power of AI
- Reduce costs and complexity
- Eradicate legacy technologies

How can we help you advance data protection and compliance?

Wherever you are in your cybersecurity journey, we at Cloudflare have the talent and expertise to guide you – particularly as trends like AI and quantum computing present new opportunities and challenges, while improving efficiency is on top of everyone's mind. We're helping organizations like yours with these challenges today, and we'd like to share our knowledge and abilities with you too.

Learn more about our solutions for educational institutions, or contact us today.

1 888 99 FLARE | cloudflare.com/education