Cloudflare Technical Product Mapping for PCI DSS 4.0

How Cloudflare customers can use Cloudflare products to meet PCI DSS 4.0 requirements

Overview

The Payment Card Industry Data Security Standard (PCI DSS) initiative was established to ensure secure handling of payment card information by organizations. Developed by the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS offers comprehensive guidelines for maintaining security throughout payment card transactions.

PCI DSS builds upon the foundational principles of the original standard by incorporating contemporary security methodologies and technologies to address evolving cyber threats. It is designed to be adaptable, with ongoing updates to reflect advancements in cybersecurity practices and emerging technologies. PCI DSS aims to provide organizations with guidance on integrating modern security measures and facilitating the adoption of secure payment card processing practices.

The core documents of PCI DSS include the following:

1	Quick Reference Guide	Outlines the PCI/DSS 4.0 requirements at a high level
2	Deep Testing Framework	Defines the concepts of the program to guide and constrain the diverse implementations of the security capabilities.
3	Prioritized Approach Guide	A supplementary guide that helps users identify high risk target, and create a common language around PCI/DSS implementation and asset efforts

This document focuses on Cloudflare product mapping with the Security Capabilities Catalog. The mappings in this document are specific to where Cloudflare can help and where a product mapping is relevant.

The Security Capabilities Catalog is composed of two parts:

1	Cloudflare Positioning	Enterprise-level security capabilities that outline guiding principles for PCI/DSS use cases.
2	Technical Substantiations	Network-level security capabilities that inform technical implementation for relevant use cases.

This document highlights which PCI/DSS recommended capabilities are supported by Cloudflare.

Cloudflare Advantage

Cloudflare stands out in the PCI/DSS landscape for its unique approach to security, particularly through the introduction of its connectivity cloud. Cloudflare has been able to provide a unified platform of cloud native services designed to deliver low-latency with granular control over their internet hops, maximized security posture and digital experience, and full Layer 1 - Layer 7 architecture customization. Powered by an intelligent, programmable global cloud network, it offers unmatched security, performance, visibility and reliability for its users - in particular because it combines the best of all existing product category types in the market today (here defined as Legacy Network Providers, Specialized Clouds, and SSE vendors)

Specialized Clouds by definition do not support compliance controls across multi-cloud environments, cannot run compute and security services in a composable or unified manner with their existing capabilities, which leads to onboarding friction, security risks, and high TCO. The 'Shared Responsibility' model of compliance puts a burden on the customer to understand their entire compliance environment or face consequences from failed audits or breaches. Complex UIs and disjointed products create steep learning curves for customers who need to perform more specialized compliance tasks, and provider lock-in means adding additional cloud environments requires duplicated efforts to ensure total compliance readiness. In addition, there is an overall lack of automation when it comes to meeting data localization and residency requirements

For SSE vendors, which offer security solutions on a similar level of quality and breadth as Cloudflare, are limited due to physical factors; often times, SSE vendors have rigid networks with a limited ability to scale, and loosely integrated product sets creates poor customer experience and high opportunity cost of being locked into solutions that cannot meet all compliance requirements. In contrast, Legacy network providers (who do have the ability to scale services at a global, enterprise level) often cannot add new services in a unified or programmable manner, instead relying on bolt-on services that increase the total cost of ownership and opportunity costs due to limited business agility.

Cloudflare's connectivity cloud solution is architected for data compliance; Having elastic networking services means organizations never need to worry about growing pains, and eliminates performance bottlenecks that cost the organization money and reputation. This same network architecture is also what enables Cloudflare to apply consistent security and compliance controls on top of user and application traffic, thanks to its unified policy engine and its converged and integrated security services. Cloudflare's Data Localization suite also enables users to automate their data governance and residency across the organization, allowing them to effortlessly encrypt data and preserve end-user privacy as they comply with any local ordinances which define where traffic should be handled.

The connectivity cloud represents a unique and powerful intersection of scalable networking, security, nad privacy functionalities that would otherwise require multiple solutions to achieve the same effect. By pushing your traffic through Cloudflare's edge, you create a private network on the internet that can reach every single compliance domain you need to keep track of; when traffic enters and exits the Cloudflare network, you have the ability to apply these data compliance rules in context of wherever the data exists.

In short, since you've built your network on Cloudflare, and you're running your business on Cloudflare, you have the ability to easily adapt your organization whenever and wherever these rules happen to change.

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
Requirement 1: Install and Maintain Network Security Controls			
1.2 Network security controls (NSCs) are configured and maintained.			
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	Examples of NSCs covered by these standards include firewalls, routers with ACLs, and virtual Cloud Networks. These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network.	Cloudflare One helps users define, implement, and maintain NSCs across their environment. Once users create their private network on Cloudflare via the use of App Connectors and WAN locations, there are multiple network services products, including Gateway and Magic Firewall, that enable users to set acceptable ports and protocols across multiple identity and security posture contexts.	Customer Responsibility to ensure security policies align with business requirements. Following products can be used to implement: Gateway, Magic Firewall, Magic WAN, Tunnel
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1	Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected. To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented	Cloudflare is a SaaS managed platform where all changes and procedures are documented, maintained and followed. However it is customer responsibility to manage and follow change control process for Cloudflare services they use.	Customer Responsibility to implement proper change management procedures. Following products can be used to implement: Gateway, Magic Firewall, Magic WAN, Tunnel, WAF

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.	After onboarding and connecting their environment to Cloudflare, users can granularly define all ports and protocols permitted across their network with both its Gateway and Magic Firewall services. Public internet traffic can be filtered and stopped via WAF and associated WAF rules and API gateway using rules based on specific header information or using authentication like mTLS and JWT.	Customer Responsibility to determine services and ports that should be exposed per business requirements. Following products can be used to implement: Gateway, Magic Firewall, WAF, API Gateway
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated. If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity.	While Cloudflare can help users segment their networking environment to this standard, defining which ports and protocols should not be used is ultimately up to the customer. Security Insights can provide visibility and insights across all applications/accounts by severity and type, top insights and security optimizations that can be done. For example - unproxied domains, domains not using HTTPs, new unmanaged API endpoints, etc.	Customer Responsibility to determine services and ports that should be exposed per business requirements. Following products can be used to implement: Security Center - Security Insights, Gateway, Magic Firewall, WAF, API Gateway
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	Any file or setting used to configure or synchronize NSCs is considered to be a “configuration file.” This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely. If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.	For all Cloudflare products, NSC configuration is handled and secured on the Cloudflare Dashboard. In context of a private networking environment, Cloudflare’s services rely on users connecting and protecting their environment behind Cloudflare’s global network and administering it from a single cloud UI. With this in mind, all NSCs defined on Cloudflare are locked behind the administrator dashboard, which is presumably secured. RBAC within Cloudflare can also be used to determine which services certain administrators have access to.	For all Cloudflare products, this is handled and secured by the Cloudflare SaaS. Cloudflare Platform
1.3 Network access to and from the cardholder data environment is restricted.			
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Unauthorized traffic cannot enter the CDE. Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit “deny all” or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.	All Cloudflare products that administer and secure L4 network services use a default-deny policy, so no unauthorized traffic can enter the CDE unless the user configures it to do so. In the event that public internet traffic needs to interact with the CDE (via API calls or web transactions), Cloudflare WAF can be used to identify malicious traffic and block it from accessing the application. API gateway can be used to lockdown and secure API traffic to application.	Customer Responsibility to ensure security policies align with business requirements. Following products can be used to implement: Gateway, Magic Firewall, WAF, API Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Unauthorized traffic cannot leave the CDE. Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.	All Cloudflare products that administer and secure network services use a default-deny policy, so no unauthorized traffic can leave the CDE unless the user configures it to do so	Customer Responsibility to ensure security policies align with business requirements. Following products can be used to implement: Gateway, Magic Firewall
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.	All Cloudflare products that administer and secure network services can block unauthorized traffic to-and-from specific subnets, which in this case includes wireless subnets (controlled by the organization) and a CDE. Thanks to its default-deny policy, no unauthorized network traffic is permitted to enter a CDE	Customer Responsibility to ensure security policies align with business requirements. Following products can be used to implement: Gateway, Magic Firewall
1.4 Network connections between trusted and untrusted networks are controlled.			
1.4.1 NSCs are implemented between trusted and untrusted networks.	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.	Cloudflare prevents unauthorized traffic from traversing trusted network boundaries in context of both internal and public internet traffic - internal traffic can be managed with both SWG policies and Magic Firewall services, and public internet traffic can be filtered and stopped via our WAF and associated WAF rules and API gateway using authentication like mTLS and JWT.	Gateway, Magic Firewall, WAF, API Gateway
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	System components that provide publicly accessible services, such as email, web, and DNS servers, are the most vulnerable to threats originating from untrusted networks. Ideally, such systems are placed within a dedicated trusted network that is public facing (for example, a DMZ) but that is separated via NSCs from more sensitive internal systems, which helps protect the rest of the network in the event these externally accessible systems are compromised.	Cloudflare can restrict and filter network communications between untrusted and trusted networks - in the event that system components need to be public facing, Cloudflare can implement NSCs on inbound traffic that can meet the standards specified in this capability. For example, customers can create a WAF rule that only allows web/API requests to an application from a specific IP address or a request that has a valid MTLS certificate or JWT. Gateway and Magic Firewall can properly segment the user's internal network from any public-facing components.	Gateway, Magic Firewall, WAF, API Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Filtering packets coming into the trusted network helps to, among other things, ensure packets are not "spoofed" to appear as if they are coming from an organization's own internal network	Spoofed IP gets blocked by the Cloudflare network, so no traffic on L7 services gets through. TCP (and QUIC) involve a 2-way handshake, so spoofed IPs are stopped at the connection termination in the proxy. L3 spoofed traffic can be filtered out when using CDN or Spectrum. Spectrum terminates connections and then proxies them forward, so spoofed IP traffic never reaches the origin server. Measures can also be taken to stop spoofed packets from infiltrating a network. A very common defense against spoofing is ingress filtering, outlined in BCP38 (a Best Common Practice document). Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers. Magic Firewall can filter packets based on source IP and user can create allowed IP lists and use that for MFW to do filtering. Cloudflare also has managed lists that can block common botnet IPs, malicious IPs, etc.	Cloudflare SaaS Platform (Magic Firewall can filter at L3/L4 level and based on threat intelligence data)
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk).	Users that onboard their network to Cloudflare can manage all L3-L7 traffic that goes in or out of their environment. If the CDE is part of this environment, Cloudflare can restrict all inbound and outbound network traffic that comes from untrusted networks. Cloudflare can implement NSCs on inbound traffic that can meet the standards specified in this capability. For example, customers can create a WAF rule that only allows web/API requests to an application from a specific IP address or a request that has a valid MTLS certificate or JWT.	Gateway, Magic Firewall, WAF
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	Methods to obscure IP addressing may include, but are not limited to: • IPv4 Network Address Translation (NAT). • Placing system components behind proxy servers/NSCs. • Removal or filtering of route advertisements for internal networks that use registered addressing. • Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.	Cloudflare works as a Proxy and such can shield both public and private IP addresses. Using Cloudflare Tunnel, customers can connect servers with private IP addresses to the Cloudflare network to be made publicly accessible in a secure way while shielding IP address information. IP addresses and other identifying network information are only available to users with the appropriate level of access to the Cloudflare Dashboard, thanks to Cloudflare's ability to restrict and hide PII.	Cloudflare SaaS Platform - Proxy Cloudflare Tunnel, Cloudflare Dashboard

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.			
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, network based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network.	If users connect to both untrusted networks and the CDE, Cloudflare has multiple security controls in place to protect both the device and the network. By running the device client or otherwise on-ramping their traffic to the Cloudflare Network, users will filter their traffic via L3-L7 Gateway rules and L7 antivirus scans. If a user begins performing suspicious or malicious activity, such as failing device posture checks or triggering DLP violations, then their device can be classified as 'high risk', which can then be used to restrict access to more sensitive parts of the organization's networked environment. If a user's device is compromised, then administrators can lock down a user's device and account access across the whole organization from the Zero Trust dashboard.	Gateway, Magic Firewall, Zero Trust Dashboard
Requirement 2: Apply Secure Configurations to All System Components			
2.2 System components are configured and managed securely.			
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need	This requirement aims to ensure that different functions do not impact the security profiles of other services in a way which may cause them to operate at a higher or lower security level. Ideally, each function should be placed on different system components. This can be achieved by implementing only one primary function on each system component. Another option is to isolate primary functions on the same system component that have different security levels, for example, isolating web servers (which need to be directly connected to the Internet) from application and database servers.	Cloudflare's ZTNA solution can secure access to multiple systems running on the same server and prevent lateral movement across different services in the network. Cloudflare's SWG solution can also properly segment any and all internal network traffic, including traffic that occurs between different system components.	Customer Responsibility to ensure application design meets security requirements. Following products can be used to implement security policies and restrict access: Access, Gateway
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	There are many protocols that could be enabled by default that are commonly used by malicious individuals to compromise a network. Disabling or removing all services, functions, and protocols that are not used minimizes the potential attack surface—for example, by removing or disabling an unused FTP or web server.	Users who onboard their environment to Cloudflare can manage all inbound and outbound network traffic using L3-L7 Gateway rules. Cloudflare's SWG solution can apply 5-tuple firewall policies that restrict any ports and protocols deemed unnecessary.	Customer Responsibility to identify necessary services, protocols, daemons, and functions and remove or disable others. Following products can be used to implement: Gateway, Magic Firewall

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
2.2.6 System security parameters are configured to prevent misuse.	System components cannot be compromised because of incorrect security parameter configuration. For systems to be configured securely, personnel responsible for configuration and/or administering systems should be knowledgeable in the specific security parameters and settings that apply to the system. Considerations should also include secure settings for parameters used to access cloud portals.	Default policies for WAF Managed Rules are managed by Cloudflare and provide instant protection without any additional configuration required. Cloudflare provides the ability for customers to configure security policies via dashboard across all security products. It's customer's responsibility to ensure they are knowledgeable about configuring security services. Cloudflare provides product and configuration documentation. Cloudflare also allows for locking down dashboard and API access to authorized individuals through RBAC and two factor authentication. It also allows users to implement identity and device posture management for onboarded applications.	Customer responsibility to ensure custom rules and security policies are applied correctly for respective applications. Following products can be used to implement: Access, Gateway, Magic Firewall, WAF, API Gateway
2.2.7 All non-console administrative access is encrypted using strong cryptography.	Whichever security protocol is used, it should be configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates, supporting only strong encryption, and not supporting fallback to weaker, insecure protocols or methods. Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions. Cleartext protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.	Using the Cloudflare API for managing the Cloudflare products requires authentication so that Cloudflare knows who is making requests and what permissions the have. An API token must be created to grant access to the API to perform actions. Cloudflare uses RFC standard Authorization: Bearer <API_TOKEN> interface. Calls use TLS/SSL encryption. User traffic that is on-ramped to Cloudflare's network via WAN locations, device clients, or other methods will encrypt the traffic before sending it to Cloudflare edge. API Gateway can be used to secure application APIs. MTLS and JWT validation can be used to provide for authentication over TLS/SSL.	Customer Responsibility to ensure API tokens are stored securely and secure protocols are used. Following products can be used to implement: Cloudflare API, Cloudflare API Gateway, Magic WAN

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
Requirement 3: Protect Stored Account Data			
3.2 Storage of account data is kept to a minimum.			
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed. Methods of eliminating data when it exceeds the retention period include secure deletion to complete removal of the data or rendering it unrecoverable and unable to be reconstructed. Identifying and securely eliminating stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated, manual, or a combination of both. The deletion function in most operating systems is not "secure deletion" as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable	Cloudflare dashboard stores request log data for 30 days. WAF does not store payload data by default, but if customers enable payload logging then it will also be stored for 30 days.	Customer Responsibility to follow data retention policies/guidelines for their applications. Following products can be used to implement: Cloudflare Dashboard, WAF.
3.3 Sensitive authentication data (SAD) is not stored after authorization.			
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	The authorization process completes when a merchant receives a transaction response (for example, an approval or decline). The storage of SAD upon completion of the authorization process is prohibited.	Cloudflare security products do not retain any financial or card transaction data. Cloudflare Sensitive Data Detection can alert on sensitive data in the HTTP or API response. API Gateway has integration with Sensitive Data Detection where it alerts in the dashboard sensitive data that is being exposed on API responses.	Customer Responsibility to follow data retention policies/guidelines for their applications. WAF, API Gateway
3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.	In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.	Cloudflare security products do not retain any financial or card transaction data. Cloudflare Sensitive Data Detection can alert on sensitive data in the HTTP or API response. API Gateway has integration with Sensitive Data Detection where it alerts in the dashboard sensitive data that is being exposed on API responses.	Customer Responsibility to follow data retention policies/guidelines for their applications. WAF, API Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
3.3.1.2 The card verification code is not retained upon completion of the authorization process.	Data sources to review to ensure that the card verification code is not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.	Cloudflare security products do not retain any financial or card transaction data.	Customer Responsibility to ensure application meets security requirements.
3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	Data sources to review to ensure that PIN and PIN blocks are not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.	Cloudflare security products do not retain any financial or card transaction data.	Customer Responsibility to ensure application meets security requirements.
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography	This requirement applies to all storage of SAD, even if no PAN is present in the environment.	Cloudflare security products do not retain any financial or card transaction data.	Customer Responsibility to ensure application meets security requirements.
3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.	Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.	Cloudflare security products do not retain any financial or card transaction data.	Customer Responsibility to ensure application meets security requirements.

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
Requirement 3: Protect Stored Account Data			
3.4 Access to displays of full PAN and ability to copy PAN is restricted.			
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Applying access controls according to defined roles is one way to limit access to viewing full PAN to only those individuals with a defined business need. The masking approach should always display only the number of digits needed to perform a specific business function. For example, if only the last four digits are needed to perform a business function, PAN should be masked to only show the last four digits. As another example, if a function needs to view to the bank identification number (BIN) for routing purposes, unmask only the BIN digits for that function.	Cloudflare can redact PII that appears in user traffic, so that it does not appear in any log details.	Customer Responsibility to ensure application takes appropriate security measures for masking and storing data. Following products can be used to implement: Gateway
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.	Cloudflare RBI can also apply data protection controls on top of remote browsers to prevent users from copy/pasting, uploading, or downloading any content on a given web app or site.	Following products can be used to implement: Gateway, RBI

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Products
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks			
4.2 PAN is protected with strong cryptography during transmission.			
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	Sensitive information must be encrypted during transmission over public networks	All traffic sent to and over the Cloudflare network is encrypted with strong cryptography. Organizations that have onboarded their networking and security environments to Cloudflare will have this applied to their traffic unilaterally and automatically. For Origin servers, Cloudflare supports both RSA Elliptic Curve Cryptography (ECC) encryption.	Gateway, Magic WAN,
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Wireless networks present unique risks to an organization; therefore, they must be identified and protected according to industry requirements. Strong cryptography for authentication and transmission of PAN is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data Wireless networks should not permit fallback or downgrade to an insecure protocol or lower encryption strength that does not meet the intent of strong cryptography.	All traffic sent to and over the Cloudflare Network is encrypted with strong cryptography. Organizations that onboard their networking and security environment to Cloudflare will have this applied unilaterally and automatically to their traffic. This includes wireless networks that exist within WAN locations.	Gateway, Magic WAN,

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 5: Protect All Systems and Networks from Malicious Software			
5.2 Malicious software (malware) is prevented, or detected and addressed.			
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	Without an antimalware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. It is beneficial for entities to be aware of "zeroday" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior.	Traffic uploaded from machines using Cloudflare's device client or other traffic on-ramps will have uploads and downloads scanned using a L7 antivirus that's enforced at the Cloudflare Edge Network. Cloudflare Gateway, also enforced at Cloudflare's edge, can block traffic to websites categorized as security threats. Gateway can also isolate suspicious websites, ensuring any malware that the user encounters is restricted to an isolated browser and destroyed when the user closes the tab. Cloudflare leverages its own threat intelligence as well as external sources in order to identify web-based threats. Anti-malware protections come into play through Cloudflare's WAF Uploaded Content Scanning, and through Cloudflare's Secure Web Gateway policies that are aimed at the appropriate security categories.	Gateway, RBI, WAF Uploaded Content Scanning
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.	Traffic sent to Cloudflare's network will have uploads and downloads scanned using an L7 Antivirus service enforced at Cloudflare's edge. Cloudflare Gateway, also enforced at Cloudflare's edge, can block traffic to websites categorized as security threats. Gateway can also isolate suspicious websites, ensuring any malware that the user encounters is restricted to an isolated browser and destroyed when the user closes the tab. Users browsing in isolation can have data protection controls overlaid on top of their session, preventing them from uploading or downloading potentially harmful content altogether.	Gateway, RBI, WAF Uploaded Content Scanning
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.			
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	Anti-malware mechanisms should be updated via a trusted source as soon as possible after an update is available. Using a trusted common source to distribute updates to end-user systems helps ensure the integrity and consistency of the solution architecture. Updates may be automatically downloaded to a central location—for example, to allow for testing—prior to being deployed to individual system components	Cloudflare's antivirus software is updated on a regular basis, using internal threat intelligence gained by analyzing trillions of web requests/day, as well as several third party threat intelligence databases. Cloudflare Gateway also uses this machine-learned threat intelligence to identify and classify harmful sites that appear on the web. Cloudflare's RBI technology is similarly kept up to date.	Gateway, RBI, WAF Uploaded Content Scanning

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 5: Protect All Systems and Networks from Malicious Software			
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.			
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.	Active, or real-time, scanning checks files for malware upon any attempt to open, close, rename, or otherwise interact with a file, preventing the malware from being activated.	Cloudflare L7 Antivirus is enforced at Cloudflare's edge, and can scan uploaded or downloaded files for malware. Any detections will be blocked from the organization's security environment.	Gateway, WAF Uploaded Content Scanning
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity's network.	Malware detected and stopped by Cloudflare's L7 antivirus software will appear in traffic logs, showing users the blocked request and reason for the block.	Gateway, WAF Uploaded Content Scanning
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of antimalware solutions could allow malware to propagate unchecked and undetected. Additional security measures that may need to be implemented for the period during which antimalware protection is not active include disconnecting the unprotected system from the Internet while the anti-malware protection is disabled and running a full scan once it is re-enabled.	Cloudflare's L7 antivirus is enabled at its edge. All Cloudflare on-ramps can be configured to prevent users from disabling them. Any changes to this configuration are documented inside of admin audit logs.	Zero Trust, Magic WAN, WAF Uploaded Content Scanning
5.4 Anti-phishing mechanisms protect users against phishing attacks.			
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing.	Cloudflare Gateway uses threat intelligence gained from trillions of requests/day sent across the Cloudflare network and uses this to categorize websites as potential phishing threats.	Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 6: Develop and Maintain Secure Systems and Software			
6.3 Security vulnerabilities are identified and addressed.			
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.	Web Application Firewall (WAF) Managed Rules allow customers to deploy pre-configured managed rulesets that provide immediate protection against zero-day vulnerabilities, top 10 attack techniques, use of stolen/exposed credentials, extraction of sensitive data, etc. WAF checks incoming web requests and filters undesired traffic based on sets of rules (rulesets) deployed at the edge. These managed rulesets are maintained and regularly updated by Cloudflare. From the extensive threat intelligence obtained from across our global network, Cloudflare is able to quickly detect and classify threats. As new attacks/threats are identified, Cloudflare will automatically push WAF rules to customers to ensure they are protected against the latest zero-day attacks. Additionally, Cloudflare provides for WAF Attack Score which complements Cloudflare managed rules by detecting attack variations. These variations are typically achieved by malicious actors via fuzzing techniques trying to identify ways to bypass existing security policies. WAF classifies each request using a machine learning algorithm, assigning an attack score from 1 to 99 based on the likelihood that the request is malicious.	WAF, API Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 6: Develop and Maintain Secure Systems and Software			
6.4 Public-facing web applications are protected against attacks.			
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent webbased attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. A web application firewall (WAF) installed in front of public-facing web applications to check all traffic is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4)	When users make web requests to applications protected by Cloudflare Access, their traffic is sent to Cloudflare's edge network where it enforces identity and security posture requirements. Organizations serving their web-based applications this way can protect them from web-based threats. Web Application Firewall (WAF) Managed Rules allow customers to deploy pre-configured managed rulesets that provide immediate protection against zero-day vulnerabilities, top 10 attack techniques, use of stolen/exposed credentials, extraction of sensitive data, etc. WAF checks incoming web requests and filters undesired traffic based on sets of rules (rulesets) deployed at the edge. These managed rulesets are maintained and regularly updated by Cloudflare. From the extensive threat intelligence obtained from across our global network, Cloudflare is able to quickly detect and classify threats. As new attacks/threats are identified, Cloudflare will automatically push WAF rules to customers to ensure they are protected against the latest zero-day attacks. Additionally, Cloudflare provides for WAF Attack Score which complements Cloudflare managed rules by detecting attack variations. These variations are typically achieved by malicious actors via fuzzing techniques trying to identify ways to bypass existing security policies. WAF classifies each request using a machine learning algorithm, assigning an attack score from 1 to 99 based on the likelihood that the request is malicious.	WAF, API Gateway, Access, Gateway Cloudflare Security products can detect and mitigate attacks. It is customer responsibility to review public facing applications to ensure they align with security best practices.

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 6: Develop and Maintain Secure Systems and Software			
6.4 Public-facing web applications are protected against attacks.			
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. A web application firewall (WAF), which can be either on-premise or cloud-based, installed in front of public-facing web applications to check all traffic, is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4).	Web Application Firewall (WAF) Managed Rules allow customers to deploy pre-configured managed rulesets that provide immediate protection against zero-day vulnerabilities, top 10 attack techniques, use of stolen/exposed credentials, extraction of sensitive data, etc. WAF checks incoming web requests and filters undesired traffic based on sets of rules (rulesets) deployed at the edge. These managed rulesets are maintained and regularly updated by Cloudflare. From the extensive threat intelligence obtained from across our global network, Cloudflare is able to quickly detect and classify threats. As new attacks/threats are identified, Cloudflare will automatically push WAF rules to customers to ensure they are protected against the latest zero-day attacks. Additionally, Cloudflare provides for WAF Attack Score which complements Cloudflare managed rules by detecting attack variations. These variations are typically achieved by malicious actors via fuzzing techniques trying to identify ways to bypass existing security policies. WAF classifies each request using a machine learning algorithm, assigning an attack score from 1 to 99 based on the likelihood that the request is malicious.	Customer Responsibility to configure appropriately WAF, API Gateway
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary	Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems).	To satisfy the requirement to confirm each script is authorize, organizations can deploy Content Security Policies (CSP) headers with Page Shield on any credit card information capturing URLs, commonly are but not limited to checkout payment pages. CSPs are a form of positive security model that can be defined to allow selected JavaScripts to run on the payment pages and deny-by-default any JavaScripts not explicitly allowed. A constantly running page monitor can help generate a CSP header, and continuously check the contents of these scripts for any malicious threats. To meet the requirement to assure the integrities of each script, Page Shield provides automatic malicious detections for JavaScript files (ML classification for crypto mining, malware, and Magecart attacks; behavior analysis; and threat intelligence feeds lookup. To meet the requirement of maintaining an inventory with written justification, use Page Shield's Script Monitor plus export function, where you create a static snapshot in a CSV with written justification. This has been validated by a third-party QSA.	Page Shield

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
6.5 Changes to all system components are managed securely.			
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components	While it's the user's responsibility to define their organizational security posture, Cloudflare logs indicate any changes to system configurations that have occurred within the platform. Since Cloudflare's edge is being used as a security perimeter, users that have properly onboarded their environment to Cloudflare will have visibility over all L3-L7 activity that has occurred.	Customer responsibility to ensure changes are consist with security policy. Following products can be used to implement: Zero Trust
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.	While it's the customer's responsibility to conduct change management reviews where applicable, Cloudflare can enable users to adapt their network and security perimeter wherever it needs to change, including in the context of keeping components PCI DSS compliant.	Customer Responsibility to ensure changes are reviewed and consistent with security policy. Following products can be used to implement: API Gateway, WAF, Zero Trust, Magic WAN
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	Pre-production environments include development, testing, user acceptance testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from preproduction functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.	Cloudflare can properly segment pre-production environments from the rest of a user's network, using RBAC for different tenants within the account, using app connectors like Cloudflare Tunnel to proxy resources across the CF network, and, and security policies for onboarded subnets and applications.	Cloudflare Dashboard, Cloudflare Tunnel, Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed	The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access.	Users can properly segment pre-production environments by applying RBAC for different domains or tenants in the same account, or by applying security posture policies to applications proxied over Cloudflare Access or Gateway.	Customer Responsibility to configure appropriately Cloudflare Dashboard, Access, Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know			
7.2 Access to system components and data is appropriately defined and assigned.			
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	It is important to establish the appropriate access level for application or system accounts	Applications protected behind Cloudflare use RBAC security models. Administrator accounts for the CF platform are also defined using RBAC. All relevant accounts can be defined using least-privileged access principles..	Customer responsibility to define access policies which can be implemented using CF products. Cloudflare Dashboard, Access, Gateway
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	Regular review of access rights helps to detect excessive access rights remaining after system functions change, or other application or system modifications occur. If excessive rights are not removed when no longer needed, they may be used by malicious users for unauthorized access	While it's the customer's responsibility to review organizational access privileges, all account access privileges are documented within the Cloudflare platform.	Customer Responsibility Can be implemented with: Cloudflare Dashboard, Access, Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know			
7.3 Access to system components and data is managed via an access control system(s).			
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges.	Cloudflare Access helps users structure access to proxied applications based on identity and device posture contexts - when a user launches their applications from the CF app launcher, they will only be shown applications they are authorized for. Cloudflare can perform user activity coaching via customizable block pages, but by default users will not be directly told why they were unable to access a given system. Administrators will have full visibility over access attempts or blocked traffic, including a specific definition of what security policy the user failed. Cloudflare supports RBAC to ensure Cloudflare platform users only have access to components based on their role.	Cloudflare Dashboard, Access
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	Restricting privileged access with an access control system reduces the opportunity for errors in the assignment of permissions to individuals, applications, and systems.	Any accounts created for the Cloudflare platform or any onboarded application/subnet can be defined in context of user's job classification and permission level.	Cloudflare Dashboard, Access
7.3.3 The access control system(s) is set to "deny all" by default.	A default setting of "deny all" ensures no one is granted access unless a rule is established specifically granting such access.	Secure access to the Cloudflare platform, or any onboarded application/subnet is default-deny. Once a user defines access groups and an appropriate security posture, only those accounts will have access.	Cloudflare Dashboard, Access

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 8: Identify Users and Authenticate Access to System Components			
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.			
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	By ensuring each user is uniquely identified, instead of using one ID for several employees, an organization can maintain individual responsibility for actions and an effective record in the audit log per employee. In addition, this will assist with issue resolution and containment when misuse or malicious intent occurs.	All accounts seen across an organization's security perimeter are documented and managed in the Cloudflare Dashboard. This includes any accounts from the user's IDP, or emails from users outside of the organization who attempt to log in. All devices that these user accounts log into will be similarly documented and managed from the Dashboard. In the event of misuse or malicious activity, these accounts and associated devices can be locked down.	Cloudflare Dashboard
8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	The ability to associate individuals to the actions performed with an account is essential to provide individual accountability and traceability regarding who performed an action, what action was performed, and when that action occurred.	Cloudflare secures access to any application, subnet, or resource onboarded to its network by applying identity and device posture policies to incoming requests. The use of group, shared, or generic accounts during this authorization challenge is prevented if the request does not meet the appropriate identity and device posture requirements.	Customer responsibility to verify use of shared credentials based on web request context. Cloudflare Dashboard, Access, Gateway
8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Service providers with remote access to customer premises typically use this access to support POS POI systems or provide other remote services. If a service provider uses the same authentication factors to access multiple customers, all the service provider's customers can easily be compromised if an attacker compromises that one factor.	Cloudflare secures access to any application, subnet, or resource onboarded to its network by applying identity and device posture policies to incoming requests. Each hypothetical remote access solution for customer environments can be defined as a separate application, which can use unique authentication factors for each premises.	Cloudflare Dashboard, Access, Gateway
8.2.5 Access for terminated users is immediately revoked.	It is imperative that the lifecycle of a user ID (additions, deletions, and modifications) is controlled so that only authorized accounts can perform functions, actions are auditable, and privileges are limited to only what is required.	All accounts seen across an organization's security perimeter are documented and managed in the Cloudflare Dashboard. Any terminated user can be immediately removed from the platform, and administrators can revoke any devices that this username has been seen from.	Customer responsibility to remove terminated users. Cloudflare Dashboard

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 8: Identify Users and Authenticate Access to System Components			
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	Where it may be reasonably anticipated that an account will not be used for an extended period of time, such as an extended leave of absence, the account should be disabled as soon as the leave begins, rather than waiting 90 days.	While it's the user's responsibility to disable accounts during the appropriate time period, all user accounts seen across an organization's security perimeter are documented and managed on the Cloudflare Dashboard. Administrators can disable specific accounts at-will and prevent them from accessing any system protected by Cloudflare, even if they would normally be granted permission.	Customer Responsibility Can implement with: Cloudflare Dashboard, Access
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity	Allowing third parties to have 24/7 access into an entity's systems and networks in case they need to provide support increases the chances of unauthorized access. Enabling access only for the time periods needed and disabling it as soon as it is no longer required helps prevent misuse of these connections.	While it's the user's responsibility to disable accounts when no longer needed, all user accounts seen across an organization's security perimeter are documented and managed on the Cloudflare Dashboard. Administrators can disable specific accounts at-will and prevent them from accessing any system protected by Cloudflare. All user activity is also documented in the Cloudflare Dashboard, so administrators can monitor them for unexpected or unauthorized activity.	Customer Responsibility Can implement with: Cloudflare Dashboard, Access
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. The re-authentication can be applied either at the system level to protect all sessions running on that machine or at the application level.	All applications protected by Cloudflare can have a session duration timer set, indicating how much time needs to pass before the user needs to reauthenticate to an application.	Costumes are responsible for maintaining appropriate access configurations to Cloudflare Dashboard. Cloudflare Dashboard, Access, Gateway,
8.3 Strong authentication for users and administrators is established and managed.			
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	An account cannot be accessed except with a combination of user identity and an authentication factor.	Accounts that can access the Cloudflare Dashboard can have MFA requirements imposed on them. Accounts that can access applications proxied by Cloudflare can also have MFA requirements imposed on them via device posture elements within Access and Gateway policies.	Cloudflare Dashboard, Access, Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.			
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors.	All applications, subnets, and resources onboarded to Cloudflare's network can have MFA rules enforced as part of a secure access requirement.	Cloudflare Dashboard, Access, Gateway
8.4.2 MFA is implemented for all access into the CDE.	Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors.	All applications, subnets, and resources onboarded to Cloudflare's network can have MFA rules enforced as part of a secure access requirement.	Cloudflare Dashboard, Access, Gateway
8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	Multi-factor authentication (MFA) requires an individual to present a minimum of two of the three authentication factors specified in Requirement 8.3.1 before access is granted. Using one factor twice (for example, using two separate passwords) is not considered multifactor authentication.	All applications, subnets, and resources onboarded to Cloudflare's network can have MFA rules enforced as part of a secure access requirement.	Cloudflare Dashboard, Access, Gateway
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.			
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE.	All applications, subnets, and resources onboarded to Cloudflare's network can have MFA rules enforced as part of a secure access requirement. MFA requirements within Access or Gateway policies cannot changed except by an administrator with the appropriate level of access. Any changes made in this way will be documented in an audit log. Exceptions can be authorized based on configuration elements within the Access policy.	Cloudflare Dashboard, Access, Gateway

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data			
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.			
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	Audit logs must exist for all system components. Audit logs send alerts the system administrator, provides data to other monitoring mechanisms, such as intrusion-detection systems (IDS) and security information and event monitoring systems (SIEM) tools, and provide a history trail for post-incident investigation.	System activities, including application access, web access, and platform access, are automatically logged in the Cloudflare Dashboard. These logs can be exported to other systems for event monitoring and incident investigation.	Cloudflare Dashboard
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Accounts with administrative access are those assigned with specific privileges or abilities for that account to manage systems, networks, and/or applications. The functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions.	All administrator access to the Cloudflare Dashboard is logged and monitored.	Cloudflare Dashboard
10.2.1.3 Audit logs capture all access to audit logs.	Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having logs identify changes, additions, and deletions to the audit logs can help retrace steps made by unauthorized personnel.	Cloudflare's audit logs cannot be tampered with or deleted. Any changes to logpush jobs will similarly be logged and monitored.	Cloudflare Dashboard
10.2.1.4 Audit logs capture all invalid logical access attempts.	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user attempts to "brute force" or guess a password.	Cloudflare's audit logs track all failed access attempts, and provide a detailed breakdown of which device posture policies the request did not meet.	Cloudflare Dashboard
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	Logging changes to authentication credentials (including elevation of privileges, additions, and deletions of accounts with administrative access) provides residual evidence of activities.	Any changes to Cloudflare administrator accounts will be logged. Any changes to any security policy in Cloudflare will also be logged.	Cloudflare Dashboard
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.	Cloudflare's audit logs meet the level of detail specified in this requirement.	Cloudflare Dashboard

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data			
10.3 Audit logs are protected from destruction and unauthorized modifications.			
10.3.1 Read access to audit logs files is limited to those with a job-related need.	Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored.	RBAC allows to control Cloudflare system Audit Log access. Audit Logs Viewer role available.	Cloudflare Platform - RBAC
10.3.2 Audit log files are protected to prevent modifications by individuals.	Stored activity records cannot be modified by personnel.	Cloudflare 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. User can also enable logging of user login events and API token events. Audit logs cannot be modified.	Cloudflare Platform - Audit Logs
10.3.3 Audit log files, including those for external facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify	Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected, even if the system generating the logs becomes compromised.	Audit logs of Cloudflare dashboard and products cannot be modified. Cloudflare is a SaaS platform which performs inherent backups of system data/information. Audit Logs are retained for 18 months before being deleted. Enterprise customers can use Log Push to store Audit Logs for longer periods of time.	Cloudflare Platform - Audit Logs
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	File integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are identified. For file integrity monitoring purposes, an entity usually monitors files that do not regularly change, but when changed, indicate a possible compromise.	Audit logs of dashboard and products cannot be modified. Cloudflare is a SaaS platform which performs inherent backups of system data/information. Audit Logs are retained for 18 months before being deleted. Enterprise customers can use Log Push to store Audit Logs for longer periods of time.	Cloudflare Platform - Audit Logs

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data			
10.5 Audit log history is retained and available for analysis.			
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Retaining historical audit logs for at least 12 months is necessary because compromises often go unnoticed for significant lengths of time. Having centrally stored log history allows investigators to better determine the length of time a potential breach was occurring, and the possible system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach.	Cloudflare 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. User can also enable logging of user login events and API token events. Audit Logs are retained for 18 months before being deleted. Enterprise customers can use Log Push to store Audit Logs for longer periods of time.	Cloudflare SaaS Platform - Audit Logs Probably ZT capabilities here for audit log on cardholder data and resources.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.			
10.6.1 System clocks and time are synchronized using time-synchronization technology.	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach.	Cloudflare manages and synchronizes time across its platform for all products and services.	Customer Responsibility to perform for their application. Cloudflare SaaS Platform
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s)	Using reputable time servers is a critical component of the time synchronization process. Accepting time updates from specific, industry accepted external sources helps prevent a malicious individual from changing time settings on systems.	Cloudflare manages and synchronizes time across its platform for all products and services.	Customer Responsibility to perform for their application. Cloudflare SaaS Platform
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations.	Cloudflare manages and synchronizes time across its platform for all products and services.	Customer Responsibility to perform for their application. Cloudflare SaaS Platform

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.			
10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used)	Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE.	Alerts are shown in the dashboard as well as sent via e-mail notification. Cloudflare Status communicates all systems issues and updates: https://www.cloudflarestatus.com/ Cloudflare allows logpush to external SIEMs to allow customers to create their own detections.	Cloudflare SaaS Platform
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used)	Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE	Alerts are shown in the dashboard as well as sent via e-mail notification. Cloudflare Status communicates all systems issues and updates: https://www.cloudflarestatus.com/ Cloudflare allows logpush to external SIEMs to allow customers to create their own detections.	Cloudflare SaaS Platform
10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment.	Alerts are shown in the dashboard as well as sent via e-mail notification. Cloudflare Status communicates all systems issues and updates: https://www.cloudflarestatus.com/ As Cloudflare is SaaS, all issues are reported, documented, and investigated to resolution. Continuous monitoring, updates, and security updates are applied.	Customer Responsibility Cloudflare SaaS Platform

CAPABILITY	Description	CLOUDFLARE SUPPORT	Cloudflare Product(s)
Requirement 11: Test Security of Systems and Networks Regularly			
11.5 Network intrusions and unexpected file changes are detected and responded to.			
11.5.1 Intrusion-detection and/or intrusion prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time	Cloudflare's Intrusion Detection System (IDS) is an Advanced Magic Firewall feature you can use to actively monitor for a wide range of known threat signatures in your traffic. An IDS expands the security coverage of a firewall to analyze traffic against a broader threat database, detecting a variety of sophisticated attacks such as ransomware, data exfiltration, and network scanning based on signatures or "fingerprints" in network traffic.	Magic Firewall - IDS
11.5.1.1 Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Detecting covert malware communication attempts (for example, DNS tunneling) can help block the spread of malware laterally inside a network and the exfiltration of data. When deciding where to place this control, entities should consider critical locations in the network, and likely routes for covert channels	Cloudflare's Intrusion Detection System (IDS) is an Advanced Magic Firewall feature you can use to actively monitor for a wide range of known threat signatures in your traffic. An IDS expands the security coverage of a firewall to analyze traffic against a broader threat database, detecting a variety of sophisticated attacks such as ransomware, data exfiltration, and network scanning based on signatures or "fingerprints" in network traffic.	Magic Firewall - IDS
11.6 Unauthorized changes on payment pages are detected and responded to.			
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Many web pages now rely on assembling objects, including active content (primarily JavaScript), from multiple internet locations. Additionally, the content of many web pages is defined using content management and tag management systems that may not be possible to monitor using traditional change detection mechanisms.	Page Shield can be used to detect clients using malicious JavaScript libraries or making connections to known malicious domains or URLs. Page Shield will also detect changes to files/code being used on a site and give a JS Integrity Score to JavaScript files assessing whether the code is malicious, and will alert you on these changes. Content Security Policies (CSPs) can be deployed to enforce a positive security mode - enforcing which resources/scripts can be used and where connections from the browser can be made to. These capabilities can prevent compromised code from performing malicious behavior such as credit card skimming. Whenever third-party code changes or malicious activity occurs, you will automatically receive an alert, meaning checks are occurring continuously, meeting the "at least every seven days" requirement. Violation reports of deployed policies can also be log pushed to various destinations including Cloudflare R2. This has been validated by a third-party QSA.	Page Shield

