

Cloudflare for Cal-Secure

California's trusted partner for cyber maturity and resilience

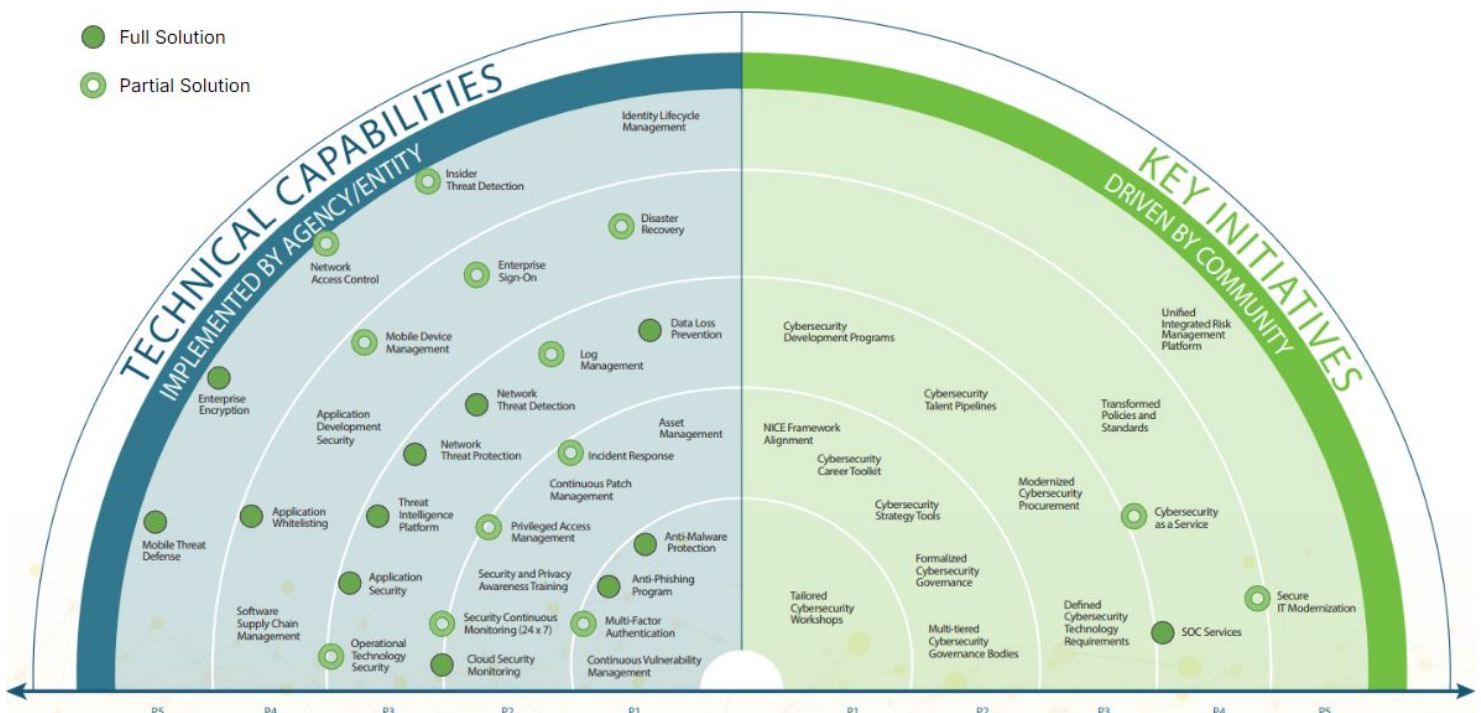


[Cal-Secure](#) is California's statewide cyber security roadmap that prepares the State for attacks of any scale. It guides Agencies to a standard baseline of cyber maturity through prioritized technical capabilities and key initiatives. The goal is strong cyber resilience to ensure the State can always serve Californians – even while under attack.

The roadmap is divided into five phases, starting with Phase 1 (P1) at the center of the Horizon Map. Agencies can choose how to implement technical capabilities – from tools they deploy themselves, cloud-based solutions, or from a select set of services offered by the California Department of Technology (CDT).

Cyber maturity requires a collaborative approach with an industry partner you can trust. That's Cloudflare.

While no cyber vendor solves everything, the green circles on the Cal-Secure Horizon Map below show where Cloudflare delivers a full solution, or contributes partially to the technical capabilities and key initiatives.



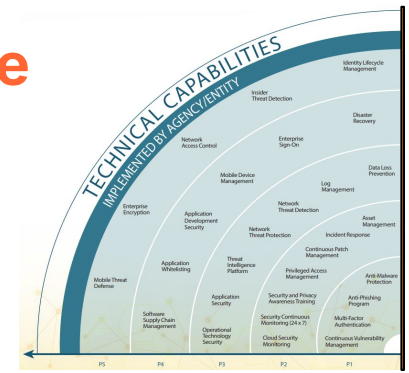
The coverage illustration shows how Cloudflare can help you acquire a significant part of your agency's required technical capabilities, but you can focus now on two of your top requirements: [Cloudflare Email Security](#) for your anti-phishing program, and [Web Application Firewall](#) for anti-malware protection.

Let Cloudflare be your trusted partner along your Cal-Secure cyber maturity journey. Keep reading for more details, or [contact us](#) today.

Technical Capabilities with Cloudflare

Technical capabilities required by Cal-Secure are on the left side of the Horizon Map, radiating outward in priority order from P1 to P5. To reach full cyber maturity, every agency across California must satisfy each one.

The table below details how Cloudflare is ready to be your trusted partner along the entire Cal-Secure maturity journey.










PRIORITY ONE

Priority	Capability	Solution	Description
P1	Anti-Malware Protection	Full ●	Cloudflare Web Application Firewall (WAF) scans application uploads to ensure that content is properly formatted and an approved file type, blocking malware from impacting your services. Cloudflare Email Security stops email-borne malware, including dangerous attachments and links that attempt to deploy malicious software on end-user devices.
P1	Anti-Phishing Program	Full ●	Cloudflare Email Security integrates with your Microsoft 365 or Google Mail services to identify and stop phishing attacks, including email-borne malware, business email compromise, and multi-channel (link-based) attacks.
P1	Multi-Factor Authentication	Partial ◉	Cloudflare Zero Trust policies can require multi-factor authentication before users can access applications, including phishing-resistant, multi-factor authentication methods that are essential for high-risk applications.
P1	Vulnerability Management		





PRIORITY TWO

Priority	Capability	Solution	Description
P2	Asset Management		
P2	Incident Response	Partial ◉	Cloudflare SOC-as-a-Service identifies suspicious activity with high confidence, leveraging our award winning threat intelligence products and Cloudflare's global network. It offers a <30 min incident response SLA, tailored mitigation guidance, and threat reporting. We also partner with incident response providers for faster recovery.
P2	Patch Management		
P2	Privileged Access Management	Partial ◉	Cloudflare Access is our Zero Trust Network Access (ZTNA) solution that integrates with our identity partners to manage and control privileged users.
P2	Awareness Training		
P2	Security Continuous Monitoring	Partial ◉	Cloudflare SOC-as-a-Service provides global, 24/7/365 protection for consistent, confident security operations that's fast and easy to start, without requiring endpoint agents or specific tools to be implemented.
P2	Cloud Security Monitoring	Full ●	Cloudflare Connectivity Cloud monitors global threats and builds intelligence into every connection — and not tied to any one cloud provider. Cloudflare proxies approximately 20% of the web, and blocks an average of ~158 billion threats per day.

PRIORITY THREE

Priority	Capability	Solution	Description
P3	Data Loss Prevention	Full 	Cloudflare DLP is a unified data loss prevention solution that protects sensitive data consistently across all networks, SaaS applications, users, and devices, while minimizing security risks and compliance issues.
P3	Log Management	Partial 	While Cloudflare is not a Log Management solution, our products generate detailed logs with that help identify security risks and create audit trails, especially when integrated with our Analytics Partnership solutions.
P3	Network Threat Detection	Full 	Cloudflare One delivers enterprise-grade network threat protection and detection in a single platform. It is our Zero Trust network-as-a-service (NaaS) solution that securely connects your remote users, offices, and data centers to each other and the resources that they need.
P3	Network Threat Protection	Full 	Cloudflare Gateway , Magic Firewall , DNS Security , DDoS Protection , Bot Management and our other critical cyber capabilities come together with Cloudforce One threat intelligence to protect your mission from sophisticated cyber attacks, detect an attack, and respond quickly and confidently.
P3	Threat Intelligence Platform	Full 	Cloudforce One delivers unparalleled threat intelligence from the power of the Cloudflare global network and our world-class threat research team. Our network processes over 60 million HTTP requests and 35 million DNS queries each second on average, providing actionable threat intelligence via STIX/TAXII standards into your security tools.
P3	Application Security	Full 	Cloudflare Application Services protects protect applications and APIs from abuse, stops bad bots, thwarts DDoS attacks, and isolates suspicious activity – all powered by built-in application services platform intelligence.
P3	OT Security	Partial 	Cloudflare security solutions can protect non-traditional devices that connect to our network, like IoT devices and other IP-enabled OT technologies.

PRIORITY FOUR

Priority	Capability	Solution	Description
P4	Disaster Recovery	Partial 	Cloudflare Connectivity Cloud enhances resilience by distributing content across a global network of servers to minimize latency, enhance performance, and increase availability. Cloudflare offers load balancing and traffic management to eliminate single points of failure.
P4	Enterprise Sign-On	Partial 	Cloudflare Access is our Zero Trust Network Access (ZTNA) solution that integrates with identity partners that validates their login against the list of allowed users and, if permitted, allows the request to proceed.
P4	Mobile Device Management	Partial 	While Cloudflare is not an MDM solution, Cloudflare MDM Partnerships include leading MDM vendors for fast deployment of our Cloudflare WARP Zero Trust client across device fleets.
P4	App Development Security		
P4	Application Allowlisting	Full 	Cloudflare Access policies determine who can reach which applications; for example, the "Allow" action allows users who meet certain criteria to reach an application behind Access.
P4	Software Supply Chain Management		

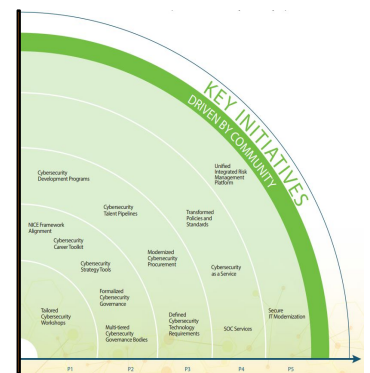
PRIORITY FIVE

Priority	Capability	Solution	Description
P5	Identity Lifecycle Management		
P5	Insider Threat Detection	Partial	Cloudflare for Unified Risk Posture monitors device behavior to help identify malicious insiders — such as users attempting to attack a corporate network or steal sensitive data.
P5	Network Access Control	Partial	Cloudflare Zero Trust Network Access (ZTNA) securely connects users to internal resources, as Zero Trust principles assume that attackers are always present on the network.
P5	Enterprise Encryption	Full	Cloudflare Connectivity Cloud encrypts all traffic across our network, and we are deploying NIST-approved Post Quantum Cryptography (PQC) to future-proof enterprise encryption.
P5	Mobile Threat Defense	Full	Cloudflare WARP protects mobile devices by securely and privately sending traffic from those devices to Cloudflare's global network, where Cloudflare Gateway can apply advanced web filtering. It also verifies device's health before it connects to your applications.

Key Initiatives with Cloudflare

On the right side of the Horizon Map, key initiatives are statewide and Agency cybersecurity ambitions for broader improvement in cyber maturity across people, process, and technology.

As your trusted technology partner, Cloudflare stands ready to help you advance your top technology-focused initiatives.



Security Operations Center Services

Provide all state entities with security operations services

[Cloudflare Security Operations Center-as-a-Service](#) is designed to meet the network and application security monitoring, threat detection and incident response needs for every Agency across the State.

We'll help you drive consistent, confident security operations for programmatic threat monitoring and response process across incident triage, investigation, and remediation – and enable state SOCs work together as a coordinated, statewide team.

Secure IT Modernization

Integrate cybersecurity into the IT Modernization Roadmap

[Cloudflare Network and Application Modernization](#) solutions make it easy to integrate cybersecurity into the state's IT Modernization Roadmap as the State begins supporting its digital services with contemporary and flexible technologies.

We'll help you consolidate, simplify, and modernize your applications, networks, and security.

Unified Risk Management Platform

Integrate risk management and automate security programs

[Cloudflare Connectivity Cloud](#) unifies security services under one control plane, providing essential security controls that help your Agency comply with regulatory requirements.

We'll also enable simple and open log management so auditors can easily follow the trail back to specific security controls to validate that they are in place and working properly.

At Cloudflare, we're ready to be your trusted partner along your Cal-Secure cyber maturity journey – and beyond.

Learn more about [Cloudflare for Public Sector](#), or [contact us](#) today.