Cloudflare Managed Defense

Expert-led threat monitoring and response

Your security team is outnumbered. Attacks are faster, more targeted, and increasingly difficult to distinguish from normal traffic noise. Most teams lack the bandwidth to review every alert, tune every rule, and respond decisively when a real incident hits — at any hour.

Cloudflare Managed Defense (CMD) closes that gap. Our Cloudforce One engineers become an extension of your team: monitoring your environment 24/7, building detection logic tailored to your specific traffic and infrastructure, and taking immediate action when real threats emerge — so your team doesn't have to.

- **Tailored detection rules:** Custom alerting logic engineered for your environment — not generic OWASP signatures or off-the-shelf thresholds.
- **Direct engagement and prioritization:** Every alert is triaged within 30 minutes, with a tracked case update sent directly to your team.
- **< 30-minute response SLA:** A contractual guarantee on urgent security incidents — not a best-effort target.
- **On-call support for active attacks:** When you're facing a critical incident, our team jumps in to investigate, recommend mitigations, and implement rules.
- **Monthly security reporting:** Regular summaries of threats detected, rules deployed, and recommendations — so you can demonstrate security posture evolution to leadership and compliance teams.

24/7 coverage without the headcount

Get continuous monitoring and expert response without hiring, training, or building an in-house security team.

Expert-grade detection from day one

CMD engineers configure tailored detection rules during onboarding. No months-long tuning cycle. No ramp-up period.

Your team, refocused on what matters

CMD handles the alerts, the false positives, and the 3am incidents. Your security team gets back to strategic work.

Cloudflare Managed Defense key features:	Core Applications	Network
Proactive monitoring & alerting for anomalous events	✓	✓
Custom, environment-tailored detection rules	✓	✓
Monthly security summary reports	✓	✓
Layer 7 attack analysis and mitigation	✓	
Layer 3 & 4 network attack analysis and mitigation		✓
Tunnel health check monitoring		✓
Supported Cloudflare Products*	• DDoS • Rate Limiting • WAF • Bot Management (*beta*) • Turnstile *(beta)*	• Magic Transit • Cloudflare Network Firewall • Advanced TCP & DNS protection

Expert-tuned detections. Direct engagement and prioritization.

Generic security tools fire alerts against textbook attack signatures — static thresholds, known CVEs, OWASP rule sets. They're not built for your traffic. CMD works differently.

Our team builds custom detection logic tailored to your specific environment — your traffic baselines, your zone configurations, your network topology. When an alert fires, CMD reviews it within 30 minutes, investigates it in the context of your environment, and opens a tracked case with a direct update to your team. You don't triage. We do.

When you're under attack or facing a critical incident, we don't send a ticket. Our team jumps in to analyze the attack in real time and implement mitigations with your approval.

This is backed by Cloudflare's global network — spanning 335+ cities, processing seven trillion HTTP/S requests and blocking 234 billion threats every day. That scale means our engineers see emerging attack patterns across the Internet before they reach your infrastructure, and can act with confidence when they do.

About Cloudforce One

Driven by a mission to help defend the Internet, Cloudforce One leverages telemetry from Cloudflare's global network — which protects approximately 20% of the web — to drive threat research and operational response, protecting critical systems for millions of organizations worldwide.

Cloudforce One