Datasheet

Cloudforce One

Cloudflare Threat Intelligence and Operations

Stronger security and greater situational awareness for security teams

Cloudforce One reduces security risk through a powerful package of security intelligence, tools, and operations to make SOC and security teams smarter, more responsive, and more secure.

- **Threat research and briefings** arm organizations with the latest insights on threat actors and TTPs targeting their industry.
- Unmatched, ready-to-consume **threat intelligence feeds** including domains, IPs, phishing sites, DNS records and more.
- Threat researchers ready to augment your team's capability with **custom RFIs** for research on any threat.

Cloudforce One makes Cloudflare's distinguished threat intelligence available to customers, to bolster SOC teams and security postures.

Advanced tools to solidify security postures

Additionally, customers get access to multiple tools to solidify security and speed investigations:

- An automated, API-driven sinkhole service.
- Cloudflare Security Center Investigate to query threat data on IPs, ASNs, URLs, and domains.
- Brand and phishing protection that notifies when important brand keywords or assets are used in attack campaigns.

Cloudforce One tiers

	Premier	Core	ENT Customers
Threat briefings and insights			
Quarterly multi-industry threat briefings	✓	✓	✓
Early access to threat research reports	✓	✓	
Threat actor profiles	✓	✓	
Industry-specific briefings	✓		
Threat data & intelligence			
New detections based on emerging threat intel/TTPs	✓	✓	✓
Open port data and banners	✓	Limited	
Historical threat data available via API and Dashboard	Unlimited	60 days	7 days
Monthly API queries for threat intel data	50,000	10,000	2500
Threat investigation portal	✓	✓	✓
Brand and phishing protection	Advanced	Standard	
Sinkhole and honeypot API access	8 IPs	2 IPs	
Threat operations			
Requests for information (RFIs)	8*	2*	

** Annual quota; additional RFIs can be added*

Cloudflare threat intelligence advantages

Threat data at Cloudflare scale

We offer differentiated threat intelligence because we analyze vast amounts of threat data nobody else has:

- Up to 48 million HTTP requests per second at peak
- 1.7+ trillion queries analyzed per day
- ~8 billion preemptive attack campaign signals per day

Exceptional threat researchers

Cloudforce One is led by our world-class threat research team, with experience analyzing threats at nation-state scale. The team's expertise spans threat research, malware/vulnerability research, and threat operations to disrupt threat actors. The team publishes briefings and reports and leads RFI processes for organizations seeking detail on threats targeting them and their industry.

Streamlined integrations

Our API-driven threat feeds easily integrate via STIX/TAXII into SOC workflows and security products like SIEM/SOAR, EDR/XDR, TIP platforms, firewalls, or security analytics. Our threat intelligence automatically protects Cloudflare customers, automatically fed into our Zero Trust suite, Magic Firewall, WAF and API Gateway.

Converting data to intelligence with layered data/threat analysis models

HTTP reverse proxy threat analysis
Attack fingerprint analysis, application attack detections, machine learning models, DDoS analysis, bot detections, TLS certificate monitoring.

DNS Analysis
DGA domain detection, DNS tunneling, newly seen/registered domains, brand protection computer vision.

Threat and infrastructure analysis
28 ML models including: malicious email content/attachments, credential harvesting sites, phishing website/spoofed domain detection, sender reputation model, BEC, malware hosting sites, IP classification, etc.

More agile SOC analysts

Security analysts gain greater context and actionable information to speed investigations. Cloudforce One provides visibility into threats via research that prioritizes important TTPs, threat experts on call to assist and our Threat Investigation Portal to provide instant context on current and historical threat data like IPs, ASNs, URLs and domains.

More effective security teams

Teams charged with bolstering the effectiveness of organizational security postures benefit from actionable threat feeds that are easily operationalized with direct STIX/TAXII integrations into security tools, to block more threats outright.

Tools like phishing protections, brand protection and sinkholes also help deliver a more effective security posture.

More confident CISOs

Security leaders reduce security risk through new intelligence that keeps organizations safer.   With security postures more effective at stopping threats before they do damage, CISOs will respond to fewer large security incidents. Additionally, they will maximize investments in security tools by arming them with distinguished threat intelligence feeds.