ITogether Service Definition Document – Cloudflare MSSP

Access Enterprise
A clientless zero trust application access service that creates an aggregation layer for identity- and context-based secure access to all your self-hosted and SaaS apps over HTTPS and SSH. It includes Cloudflare Tunnel to connect users faster and more safely than a VPN. It includes Cloudflare's standard DNS public hostname and DDoS protection services when reverse proxying connections. It includes Cloudflare mTLS to optionally secure connections with mutual TLS authentication. Refer to our general account limits for cloudflared, root certificates, and more

Gateway Enterprise
A cloud-native secure web gateway service supporting a wide range of clientless and client-based deployment modes to protect distributed offices and remote workers against ransomware, phishing, and other threats using L4-7 network, DNS, and HTTP filtering policies for faster, safer Internet browsing. It includes Cloudflare WARP device clients and Cloudflare 1.1.1.1 privacy-first DNS resolution.

Advanced Browser Isolation
A client-based or clientless remote browser isolation service that layers additional threat defence and data protection controls across browsing activities with web, SaaS and private apps. Insulates local devices from malicious code and insulates application data in use from local devices by running all browser code and rendering all browser data on Cloudflare's global network. There are no caps on usage.

Area 1 Enterprise (Email)
A cloud-native email security service supporting a wide range of inline, API-driven, and multi-mode deployments to protect inboxes against email-borne malware, business email compromise (BEC), and multi-channel (link- and QR-based) phishing attacks. The Enterprise (vs Advantage) license adds time-of-click analysis and email link isolation with more reporting and remediation capabilities.

Zero Trust Essentials PLUS
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, inline CASB, and multi- mode cloud email security (CES) capabilities to protect employees with secure access

and threat defence across web, SaaS, and private applications — extending threat defence to any email inbox including those commonly part of SaaS suites.

The PLUS license adds Cloudflare Area 1 Advantage to the Cloudflare Access and Cloudflare Gateway bundle — that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

Zero Trust Advanced PLUS
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, inline CASB, and multi- mode cloud email security (CES) capabilities to protect employees with secure access and threat defence across web, SaaS, and private applications — extending threat defence to any email inbox including those commonly part of SaaS suites. The PLUS license adds Cloudflare Area 1 Enterprise to the Cloudflare Access and Cloudflare Gateway bundle — that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

Zero Trust Premier PLUS
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, managed multi-mode cloud email security (CES), multi-mode CASB, DLP, and RBI capabilities to protect employees with secure access, maximum threat defence, and maximum data protection across web, SaaS, and private applications — extending threat defence to any email inbox including those commonly part of SaaS suites. The PLUS license further adds Cloudflare Area 1 PhishGuard to the Cloudflare Access, Cloudflare Gateway, Cloudflare CASB, Cloudflare DLP, and Cloudflare Browser Isolation bundle — that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

Zero Trust Essentials
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, and inline CASB capabilities and supports a wide range of clientless and client-based deployment modes to protect employees with secure access and threat defence across web, SaaS, and private applications. It bundles Cloudflare Access and Cloudflare Gateway — that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

Zero Trust Advanced
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, multi-mode CASB, and DLP capabilities and supports a wide range of clientless and client-based deployment

modes to protect employees with secure access, threat defence, and data protection across web, SaaS, and private applications. It further bundles Cloudflare CASB and Cloudflare DLP with Cloudflare Access and Cloudflare Gateway - that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

Zero Trust Premier
A natively-integrated security service edge (SSE) that combines ZTNA, SWG, multi-mode CASB, DLP, and RBI capabilities and supports a wide range of clientless and client-based deployment modes to protect employees with secure access, threat defence, and maximum data protection across web, SaaS, and private applications. It further bundles Cloudflare Browser Isolation with Cloudflare Access, Cloudflare Gateway, Cloudflare CASB, and Cloudflare DLP — that also includes Cloudflare WARP, Cloudflare Tunnel, and Cloudflare mTLS.

CDN/DDOS/WAF/DNS
A version of the publicly available Business Plan, this version is available exclusively to Authorized MSSP Partners. Cloudflare's Business Plan PLUS offers a range of features and benefits that make it an attractive choice for clients who want enhance security to protect against DDoS attacks and implement a Web Application Firewall (WAF).

Contact

Name	Role	Tel	Email
Tim Ripper	Account Director	0113 341 0123	tim@itogether.co.uk
Simon Richardson	Director	0113 341 0123	simon@itogether.co.uk