ARCTIQ + CLOUDFLARE

Mid-Market: Enterprise Security, Right-Sized For You

Accelerate your secure cloud adoption with Arctiq and Cloudflare

Better Together: Closing the Capability Gap

For mid-market organizations, the challenge isn't just selecting the best technology; it's having the bandwidth to get the most out of your investment. Our team bridges the gap between Cloudflare's global network and the customer's specific business need with technical skill only available in-house at the enterprise. We provide hands-on engineering capability and potentially 24/7 eyes-on-glass to create a complete defensive posture.

The Business Case: Scaling Without the Growing Pains

The Scenario: A national destination retailer is driving extensive growth through its online retail presence. At the same time, it faces not just performance bottlenecks but also an increasingly threatening landscape: AI bots, increasing DDoS threats, and global threat actors looking for ways in. Their lean IT team is agile and capable but doesn't have the bandwidth to model, implement, and evaluate the impact of a complex WAF and CDN environment.

The Arctiq Solution: Arctiq steps in to protect and accelerate the Customer's web edge just before one of their busiest shopping days of the year. We automate the configuration and deployment of Cloudflare, model firewall rules that are designed for their specific site, and offload security monitoring of their WAF to our managed SOC.

The Outcome: Internal teams can focus on improving site performance and capability while Arctiq ensures the platform remains secure and widely available – delivering peace of mind and reduced operational burden.

	Onboarding/Migration	Cloud Security Resident Architect	Managed Security for Cloudflare
What it is	A rapid-deployment engagement to get you onto Cloudflare fast. We assess your current web traffic, migrate DNS, and configure core WAF rulesets.	An Arctiq expert embeds with your team to establish governance, tune policies, and help you manage Cloudflare as part of your security environment.	Arctiq monitors your Cloudflare environment, responding directly to threats and helping you tune and optimize your environment.
Value	We replace "default settings" with "best practices" from Day 1. This service eliminates the learning curve, ensuring your web applications are protected against the OWASP Top 10 and optimized for speed immediately upon cutover.	This empowers your team to own the platform long-term. We don't just fish for you; we teach you to fish, establishing the "Infrastructure as Code" workflows that allow for consistent, reproducible security policies.	We filter the signal from the noise and give you the comfort to sleep at night. Whether it's responding to threats right away or helping you tune your environment, we help you drive the most value from your WAF.

Enterprise: Resilience & Security for Hybrid and Multi-Cloud Environments

Unify your legacy, on-prem, and multi-cloud infrastructure with Cloudflare and Arctiq.

Better Together: The Integrator for Hybrid Reality

Enterprise environments are rarely simple. They're a mix of on-premises data centers, multiple clouds, SaaS tools, and remote workers. Arctiq's key value is our ability to knit Cloudflare into this complex fabric. With Cloudflare's connectivity cloud, Arctiq can help modernize and secure your ingress without disrupting your critical business. We treat the entire Cloudflare infrastructure as code, ensuring that even the most complex hybrid environments are manageable, auditable, and compliant.

The Business Case: Modernizing the Edge

The Scenario: A large telecommunications provider has multiple legacy datacenters scattered across the country burdened by expensive, hardware-based legacy WAF appliances. They don't have the bandwidth to protect against modern threats and require complex and failure-prone DNS-based load balancing to manage resiliency. They need to modernize, but can't simply turn off their legacy environments.

The Arctiq Solution: Arctiq advertises the customer's existing IP addresses from Cloudflare's edge network and implements Magic Transit to flow that traffic directly back to the customer's backend services, shifting protection to Cloudflare's resilient cloud and providing highly resilient load-balancing capability – transparently.

The Outcome: The enterprise sheds expensive on-premises firewall hardware, achieves a unified security posture across their datacenters, makes migration to the cloud application transparent, and satisfies their compliance and audit requirements through granular, code-based policy management.

	Legacy WAF Migration	Modernizing The Hybrid Cloud	Enabling Zero Trust
What it is	We help you migrate from your existing WAF and bring automated configuration deployment to Cloudflare.	Ease your application modernization journey by centralizing your load balancing, ingress, and security in Cloudflare's edge.	A strategic rollout of Cloudflare Access and Gateway to replace legacy VPNs. We integrate with your existing Identity Providers (IdP) and define granular access policies.
Value	De-risk your digital transformation as you move to a true cloud-native hybrid edge while unlocking cost savings and performance gains.	Cloudflare's "network firewall as a service" simplifies your network architecture, provides massive DDoS mitigation capacity, and dramatically simplifies Hybrid and multi-cloud deployments or migrations.	Secure your workforce and third-party contractors without the performance penalty of backhauling traffic or expensive on-premises hardware. Per-user billing makes scalability a breeze and integrates natively with Cloudflare's hybrid cloud networking.

Partnership in Action

Whether you're protecting a voter registration portal, streamlining EDU campus WAN redesigns, or modernizing your DMZ without downtime, Arctiq + Cloudflare is the team to call.

▶ Let's make your edge secure, performant, and future-proof.

Book a Consultation