SOLUTION BRIEF

CLOUDFLARE
AREA 1 SECURITY

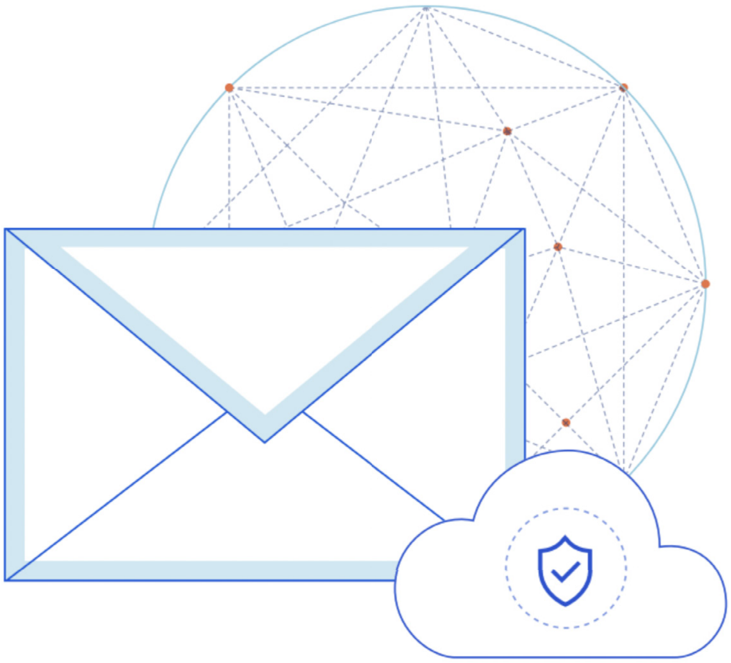
Cloud Email Security Service Resiliency

Ensure business continuity with Cloudflare Area 1 Security

As the #1 SaaS application, email is mission-critical for all businesses. As the entire world embraced digital transformation seemingly overnight, email has become the lifeblood of communication across organizations large and small, allowing for business continuity despite widespread uncertainty.

With email already the preferred threat vector for attackers, it's essential that your cloud email security service both protect against threats and provide the necessary resiliency, availability, and scalability required to conduct business. In short, today's email requires modern, cloud-native email security that can handle cloud workloads and modern attacks.

From our inherent architecture to our core features, Cloudflare Area 1 Security's cloud-native service has been designed to maintain industry-leading high availability and operational resilience, so that customers' business operations are not impacted by outages. Through features like Adaptive Message Pooling, Area 1's dynamically scalable service is capable of handling massive message spikes to make sure benign emails reach inboxes while blocking email, web, and social media-based threats.



The challenge:

Businesses suffer when mission-critical emails get delayed or disrupted due to unforeseen circumstances.

Solution:

Cloudflare Area 1 Security's cloud-first, on-demand scalable infrastructure and feature designs ensure business continuity with continuous email flow.

Operational resilience with enterprise-class high availability

Area 1 has upheld a long track record of reliability and holds our service to enterprise-class high availability. Our service has consistently maintained annual rates of five-nines availability to meet the needs of the most demanding global organizations.

Area 1's true cloud-scale, multi-tenant service is purpose-built to handle the demands of today's email traffic and address anomalous events that can overwhelm legacy architectures, all while preemptively protecting against phishing and other email, web and social-media based threats.

Area 1 is a multi-tenant, cloud-native service built on a combination of Amazon Web Services (AWS) and Google Cloud Platform (GCP). Our provider-diverse and geographically-diverse cloud service covers multiple continents, including regions in the Eastern and Western United States and Europe. Each region also includes multiple availability zones, so we're capable of automatic load-scaling with seamless fail-overs.

We don't just rely solely on cloud providers for availability. Our customers rely on us to keep their mail flowing, so redundancy is built into the Area 1 email security service itself. With native fault tolerance and extensive fail-over capabilities, Area 1 continues to run even if a given cloud provider's region is down. We also perform continuous self-monitoring so that our automated systems are aware of potential issues and can proactively adjust accordingly.

Adaptive Message Pooling:

- Autoscales TCP connections and SMTP traffic to handle massive message spikes
- Addresses TLS-heavy traffic mix seen within internet SMTP traffic
- Continuous load and queue monitoring with proactive notifications in the event of anomalous spikes
- Automatically pools/ queues messages for extended periods of time and throttle delivery post-spike events consistent with the downstream system's ability to absorb the volume
- Accounts for 'downstream' gateway unavailability, system misconfigurations, or email DoS attack

Ensuring business-critical email flow

To ensure high availability and uninterrupted email flow for our customers, the Area 1 service accounts for unforeseen circumstances like service provider outages, as well as the common but erratic traffic spike. Traffic spikes could be due to factors ranging from planned business reasons (e.g. traffic rush during seasonal events), to intentional denial of service (DoS) attacks (e.g. SMTP flood attacks), to the frequent scenario of errant applications inadvertently overwhelming mailboxes with application messages delivered over SMTP.

To address these and similar scenarios, Area 1 includes the ability to automatically pool messages using Adaptive Message Pooling, dynamically adjusting resources and provisioning additional TCP connection clusters to handle traffic and message spikes while ensuring that an organization's email traffic remains unaffected. Our customers are able to proactively assess and monitor the system's availability through these events.

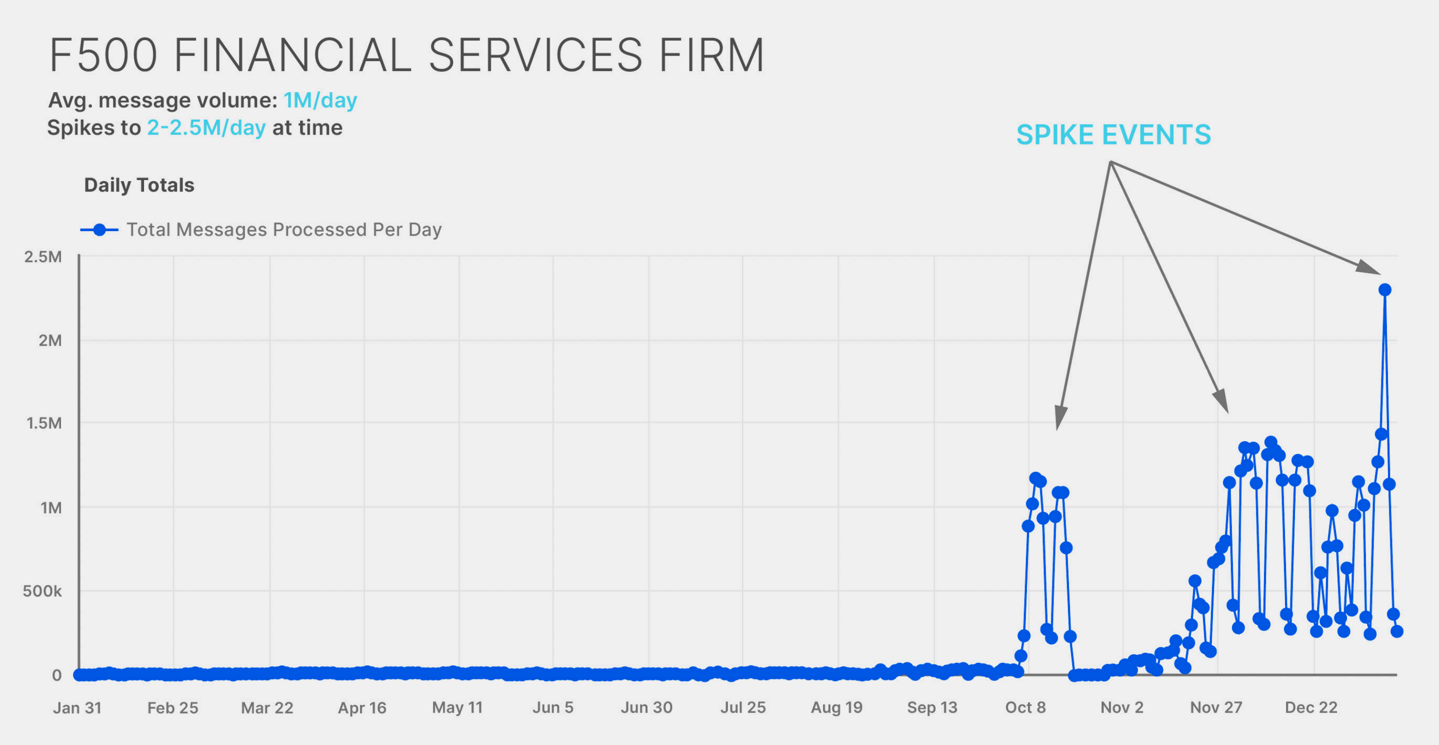
In contrast to some legacy Secure Email Gateways (SEGs) that cannot keep up with these unpredictable spikes due to their appliance-based architecture, Area 1's Adaptive Message Pooling's autoscaling of TCP connects and SMTP traffic and automatic queuing can help account for — and mitigate — downstream gateway unavailability.

Adaptive Message Pooling case study - Fortune 500 organization

A large, global Fortune 500 financial services organization typically receives a message volume of 1 million per day. During spike events, message volumes can more than double to 2.5 million messages per day. While some spike events can be anticipated, a large majority of these events are unplanned. With their legacy cloud-hosted Secure Email Gateway, the organization was struggling to deal with these spikes, leading to widespread email delays and bounce-backs, significantly impacting business.

The customer deployed Area 1 in front of their existing gateway, allowing Area 1 to handle incoming email traffic from the Internet. Now, when spike events occur, additional TCP connection clusters are provisioned and messages are automatically pooled. When the event subsides, Area 1 requeues and delivers messages at a rate which downstream systems are available to process and absorb.

By deploying Area 1, the customer is able to address traffic spikes in a seamless manner, while ensuring the highest levels of security for their organization.



The Cloudflare network - security, performance, and reliability for the modern enterprise

The Cloudflare network itself is built for tomorrow's applications. Cloudflare is the "world's network" — and it is one of the biggest, most connected, and fastest networks. It operates within 50 ms of 95% of users on the planet, so users have the same experience regardless of where they are located.

Cloudflare connects to almost every other major network in the world, so users and applications — including email — can come closer and communicate at the speed of light. We have data centers in 275+ cities in 100+ countries, including mainland China — every time our footprint grows, your global reach does as well. We standardized our hardware and software stack so that every service can run in every location, meaning that your application traffic never has to take the scenic route. And then we built a fiber-optic backbone network to increase capacity and better control the user experience.

Security without tradeoffs

Unmatched threat intelligence	Exceptional performance	High resiliency	Safeguarding customer data
Cloudflare serves millions of websites and processes vast amounts of traffic daily, giving us exceptional insights into active security threats.	With data centers in 275 cities in 100+ countries, Cloudflare is within 50 milliseconds of 95% of the world's Internet-connected population.	With our Anycast architecture and direct interconnections to 11,000 major networks, Cloudflare minimizes single points of failure and offers a highly resilient network platform with a 100% uptime SLA.	Cloudflare builds data privacy into everything we do, giving our customers control over their information and making it easier to comply with regional data privacy regulations.

The Cloudflare network - security, performance, and reliability for the modern enterprise

Today's cloud-based email environments require modern solutions for resiliency from outages, traffic spikes, and threat actors. Organizations should invest in email security with the following characteristics in order to ensure resiliency from business disruptions.

HIGH SCALE CLOUD MTA

On demand scalability with the highest levels of service assurances & adaptive message pooling

ENTERPRISE-GRADE EMAIL HYGIENE

Enforce Inbound TLS, Email Authentication, & Partner communications policies

BEST-OF-BREED ATTACK PREVENTION

Stop phishing, targeted attacks, BEC, ransomware, spam, viruses, backscatter attacks, and more

MULTI-MODE DEPLOYMENTS

Flexibility for inline, out-of-band, API / Connector for internal & inbox-based protections

QUICK VISIBILITY & DEEP CONTEXT

Rapid-scale message tracing & detections search; industry's fastest indexing & retrieval rate

OPERATIONAL SIMPLICITY & CLOUD NATIVE

Cloud-first, API-first architecture with deep hooks into existing operational tools & playbooks

Customers place enormous trust and responsibility in Cloudflare in processing their mission-critical business applications. Whether you're just transitioning to a hybrid cloud environment or already well along the digital transformation journey, Area 1 can help ensure your email is secure and resilient.

Learn more about the Area 1 email security service, which is part of Cloudflare Zero Trust platform, here.

To learn more about what the Cloudflare network can do for your business, contact enterprise@cloudflare.com.