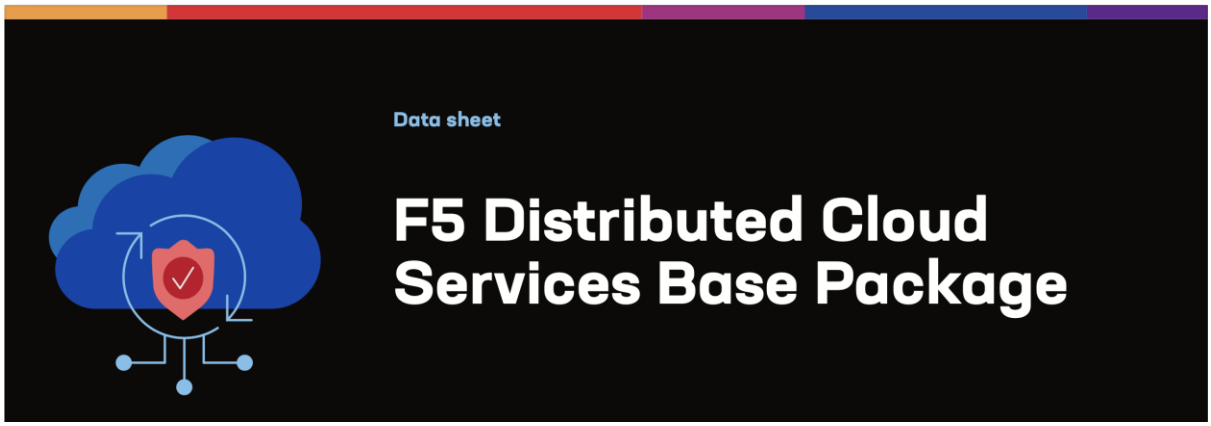
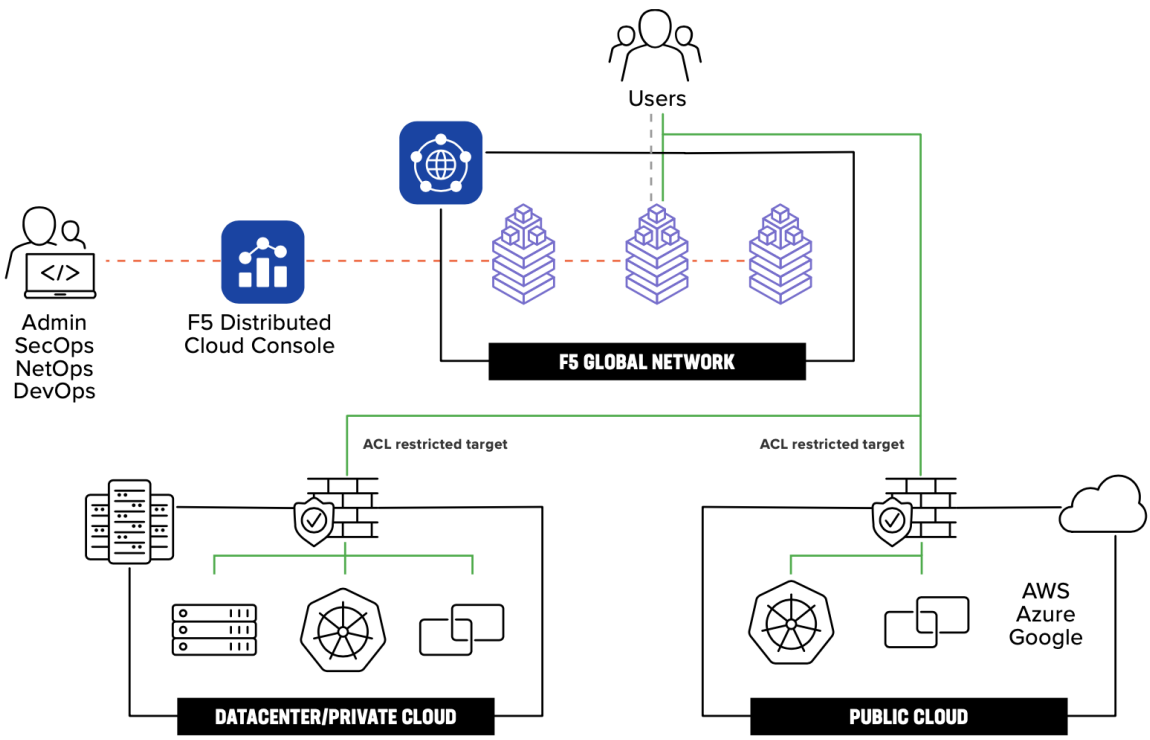


Sicurezza per Applicazioni WEB ed API accessibili al pubblico

Il base package F5® Distributed Cloud Services è un insieme di funzionalità offerte su Piattaforma cloud distribuita di F5. Questo pacchetto include un'architettura distribuita e fornisce ai clienti gli strumenti necessari per proteggere le applicazioni con il servizio F5 Distributed Cloud Web App and API Protection (WAAP). Si basa su un modello SaaS, sfruttando proxy per gestire il flusso di traffico di applicazioni WEB ed API tra client su Internet e i POP Regional Edge (RE) della rete globale F5. Applicando servizi e policy di sicurezza, gli attacchi vengono intercettati prima che minaccino le applicazioni protette, le API ed in modo più ampio la rete del cliente protetto.

Questo approccio proattivo protegge le infrastrutture applicative ed API dal traffico malevolo prima che possa raggiungere l'infrastruttura del cliente, risultando un ambiente più sicuro, migliorando le prestazioni complessive e consentendo un risparmio sui costi di infrastruttura e larghezza di banda.



Il servizio include:

Web Application Firewall

Globally-distributed load balancer: Numero illimitato di endpoint (ovvero server di origine). Numero illimitato di health check per endpoint. La granularità degli health check per gli endpoint è di un secondo.
Signature-based protection: Mitiga le vulnerabilità delle applicazioni e delle API con la tecnologia WAF di F5, supportata dal motore di analisi avanzato contenente oltre 8.000 firme per CVE, vulnerabilità e tecniche di attacco, comprese firme per bot specializzate.
Threat campaigns: Fornisce protezione contro sofisticate campagne di attacco multi-vettore tramite firme completamente controllate e sviluppate dai ricercatori F5.
Compliance enforcement: Combinazione di controlli per violazioni, tecniche di evasione e controlli di conformità del protocollo HTTP.
Automatic attack signature tuning: Modello AI ad autoapprendimento che sopprime trigger per falsi positivi.
Mask sensitive parameters or data in logs: Gli utenti possono mascherare i dati sensibili nei log delle richieste specificando nomi di Header HTTP, nomi di cookie o nomi di parametri delle query. Solo i valori sono mascherati. Per impostazione predefinita, i valori dei parametri di query card, pass, file .pwd e password sono mascherati.
Custom blocking pages and response codes: Quando una richiesta o una risposta viene bloccata dal WAF, gli utenti possono personalizzare la pagina di risposta al blocco fornita al client.
Allowed responses codes from origin: L'utente può specificare quali codici di stato della risposta HTTP sono consentiti.
IP reputation: Analizza le minacce IP e pubblica un set di dati dinamico di milioni di indirizzi IP ad alto rischio gestiti da F5 per proteggere gli endpoint delle app dal traffico in entrata proveniente da IP malevoli. Le categorie di minacce IP includono Sorgenti spam, exploit Windows, attacchi Web, botnet, Denial of Services, Scanner, Phishing e altro ancora.
Sensitive data protection for apps: Data Guard impedisce alle risposte HTTP e HTTPS di esporre informazioni sensibili, come numeri di carte di credito e numeri di previdenza sociale, mascherando i dati.
Exclusion rules: Regole che definiscono gli ID di firma e le violazioni o i tipi di attacco che devono essere esclusi dall'elaborazione WAF in base a criteri di corrispondenza specifici. I criteri di corrispondenza specifici includono dominio, percorso e metodo. Se la richiesta del client soddisfa tutti questi criteri, il WAF escluderà l'elaborazione per gli elementi configurati nel controllo di rilevamento.
CSRF protection: Consente agli utenti di configurare o specificare facilmente i domini di origine appropriati e consentiti.
Cookie protection: La protezione dei cookie offre la possibilità di modificare i cookie di risposta aggiungendo gli attributi SameSite, Secure e HTTP Only.
GraphQL protection: Il motore WAF esamina le richieste GraphQL per individuare eventuali vulnerabilità e bloccherà il traffico in base al database delle firme F5.

DDoS Mitigation

Fast ACLs: I controlli del firewall di rete consentono agli utenti di bloccare il traffico in entrata da origini specifiche o di applicare limiti di velocità al traffico di rete. Le protezioni avanzate consentono di filtrare il traffico in base a indirizzo di origine, porta di origine, indirizzo di destinazione, porta di destinazione e protocollo. Ciò include 100 prefissi IP inclusi e funzionalità di policy.
Layer 3–4 DDoS mitigation: mitigazione di attacchi volumetrici Multi-layered. Ciò include una combinazione di regole di mitigazione preimpostate con mitigazione automatica e scrubbing avanzato di mitigazione del Denial of Service (DDoS) distribuito per i clienti che utilizzano solo i servizi cloud distribuiti F5. La piattaforma protegge i servizi forniti sulla rete F5 dagli attacchi DDoS.
Layer 7 DoS detection and mitigation: Rilevamento di anomalie e avvisi su modelli e tendenze di traffico anomali tra app ed endpoint API. F5 sfrutta l'apprendimento automatico avanzato per rilevare picchi, cali e altri cambiamenti nel comportamento di App ed API nel tempo, analizzando i tassi di richiesta, i tassi di errore, la latenza e il throughput e con la possibilità di negare o limitare gli endpoint includendo la mitigazione automatica.

Layer 7 DoS policy-based challenges: È possibile impostare challenge/response personalizzate basate su policy per eseguire JavaScript o Captcha. Definire criteri di corrispondenza e regole per l'attivazione di challenge in base all'IP di origine e alla reputazione, agli ASN o alle etichette (ad esempio, città, paesi). Ciò aiuta a filtrare gli aggressori che tentano di eseguire un attacco da client legittimi. Include 200 regole di Service Policy.
Slow DDoS mitigation: Gli attacchi "Slow and Low" vincolano le risorse del server, non lasciandone nessuna disponibile per soddisfare le richieste degli utenti effettivi. Questa funzionalità consente la configurazione e l'applicazione dei valori di timeout della richiesta e degli Header della richiesta.

API Security

Signature-based protection: F5 Distributed Cloud WAF supporta l'ispezione dei due protocolli API più popolari: GraphQL e REST.

Bot Defense

Signature-based protection: Il motore delle firma WAF include firme univoche per minacce automatizzate e tecniche bot, inclusi crawler, attacchi DDoS, attacchi DoS e altro ancora.
Client-side defense: Fornisce protezione multifase per le applicazioni Web contro Formjacking, Magecart, digital skimming e altri attacchi JavaScript dannosi. Questo sistema di protezione multifase include rilevamento, avvisi e mitigazione, con 1 milione di transazioni incluse.

App Connect

End-to-end-encryption: Encryption TLS nativa per tutti i dati in transito sulla rete.

Network Connect

Multicloud transit: Transito di rete di livello 3 tra cloud pubblici, data center locali e siti edge distribuiti.
Security service insertion: Integra servizi firewall di rete esterni, come F5 BIG-IP e Palo Alto Networks, su più reti cloud.
Network segmentation: Isolamento granulare della rete e microsegmentazione per proteggere i segmenti di rete on-premise e su reti cloud pubbliche.
End-to-end-encryption: Crittografia TLS (Transport Layer Security) nativa per tutti i dati in transito sulle reti.
Automated provisioning: Provisioning e orchestrazione automatizzati di strutture di rete cloud pubbliche.
Traffico: verso Internet o la rete del cliente.

DNS (250 primary and/or secondary zones included)

Automatic failover: Garantisci un'elevata disponibilità degli ambienti DNS con un failover fluido al servizio F5 Distributed Cloud DNS.
Auto-scaling: Scala automaticamente per stare al passo con la domanda man mano che il numero di applicazioni aumenta, i modelli di traffico cambiano e i volumi delle richieste crescono.
DDoS Protection: Previeni gli attacchi DDoS o la manipolazione delle risposte del dominio con la protezione integrata.
DNSSEC: Estensione DNS che garantisce l'autenticità delle risposte DNS, inclusi i trasferimenti di zona. Restituisce inoltre risposte di negazione dell'esistenza che proteggono la rete dagli attacchi al protocollo DNS e ai server DNS.
TSIG authentication: Automatizza i servizi con API dichiarative e una GUI intuitiva.
API support: Chiavi di firma della transazione (TSIG) che autenticano le comunicazioni sui trasferimenti di zona tra client e server.

DNS Load Balancer (50 included)

Global location-based routing: Indirizza i client all'istanza dell'applicazione più vicina con bilanciamento del carico basato sulla geolocalizzazione per la migliore esperienza utente.
Intelligent load balancing: Dirige il traffico delle applicazioni tra ambienti, esegue controlli di integrità e automatizza le risposte. Include il ripristino di emergenza completamente automatizzato.
API support: Automatizza i servizi con API dichiarative e una GUI intuitiva.

ADC telemetry: Tieni traccia delle prestazioni, dello stato delle app e dell'utilizzo con la visualizzazione di base.
Multi-faceted security: La sicurezza dinamica include failover automatico, protezione DDoS integrata, DNSSEC e autenticazione TSIG.
Health checks: I controlli sui server di origine forniscono risposte in base alla disponibilità dell'applicazione. Include 200 controlli health checks.

Observability

Reporting, rich analytics, and telemetry: Visibilità unificata dall'applicazione all'infrastruttura fornita attraverso deployment edge e cloud eterogenee, incluso lo stato dei deployment delle applicazioni, l'integrità dell'infrastruttura, la sicurezza, la disponibilità e le prestazioni.
Security incidents: Vista eventi che raggruppa migliaia di singoli eventi in incidenti di sicurezza correlati in base al contesto e alle caratteristiche comuni. Mirato a semplificare l'indagine sugli eventi di sicurezza delle app.
Security events: Visualizzazione dashboard unica che consolida tutti gli eventi di sicurezza nell'intera gamma di funzionalità di sicurezza delle applicazioni Web e delle API con personalizzazione e analisi approfondita di tutti gli eventi di sicurezza WAF, bot, API e altri eventi di sicurezza di livello 7.
Global Log Receiver - Log export integration: Distribuzione dei log a sistemi di raccolta log esterni tra cui Amazon S3, Datadog, Splunk, SumoLogic e altri. Questa funzionalità include due configurazioni.
Synthetic monitoring: Monitora facilmente le tue applicazioni e i tuoi sistemi critici da regioni di tutto il mondo. Correla rapidamente i problemi di prestazioni e disponibilità a una regione o posizione specifica. Sfrutta i report TLS integrati per quantificare il rischio di scadenza dei certificati, valutare l'uso di protocolli e crittografie vulnerabili e determinare il punteggio TLS complessivo per i tuoi endpoint monitorati. Ricevi avvisi pertinenti prima che i tuoi clienti inizino a chiamare e identifica chiaramente se sono stati interessati durante l'ultima finestra di modifica o interruzione. Comprende 500mila esecuzioni.
Metrics: 30 giorni
Request logs: 7 giorni
Audit logs: 30 giorni
Alerts and notifications: Policy rules

Supporto

24/7/365 support: Il supporto viene fornito in vari metodi, tra cui ticketing della console, e-mail e supporto telefonico.
Uptime SLAs: 99.99%
Security logs: 30 giorni
Response SLA: 1 ora
Onboarding: Customer Success Team ed accesso ai training

Altro

Service policies: Abilita la microsegmentazione e supporta la sicurezza avanzata a livello di applicazione con lo sviluppo di elenchi consentiti/negati, filtraggio IP geografico e creazione di regole personalizzate per agire sulle richieste in entrata, inclusi criteri di corrispondenza e di vincolo di richiesta basati su una varietà di attributi e parametri come TLS fingerprinting, area geografica/paese, prefisso IP, metodo HTTP, percorso, intestazioni e altro.
CORS policy: Cross-Origin Resource Sharing (CORS) è utile in qualsiasi situazione in cui il browser, per impostazione predefinita, non consente richieste multiorigine, consentendo se necessario una specifica necessità di abilitarle. La policy CORS è un meccanismo che utilizza intestazioni HTTP aggiuntive per informare un browser di consentire a un'applicazione Web in esecuzione su un'origine (dominio) di avere l'autorizzazione per accedere a risorse selezionate da un server su un'origine diversa.
Trusted client IP headers: Identificazione degli indirizzi IP dei client reali per il monitoraggio, la registrazione e la definizione di policy di autorizzazione/negazione. Quando questa funzione è abilitata, gli eventi di sicurezza e i registri delle richieste mostreranno l'indirizzo IP del client reale come l'IP di origine.
Mutual TLS: Supporto sia per TLS che per Mutual Transport Layer Security (mTLS) per l'autenticazione con autorizzazione basata su policy sul bilanciatore del carico. Il proxy offre la capacità di applicare la sicurezza

end-to-end del traffico delle applicazioni. Il Mutual TLS supporta la possibilità di inviare i dettagli del certificato client ai server di origine nelle intestazioni delle richieste x-forwarded-client-cert.

Administration: numero di utenti illimitato.
Single Sign On
Role Based Access Control

Global Anycast: VIPs inclusi in base all'offerta commerciale