FIDOGROUP
BV TECH

Allegato Tecnico

Servizi Akamai per il Cliente

SAPIENZA
UNIVERSITÀ DI ROMA

Ludovica Gualdi Account Manager Ludovica.gualdi@bvtech.com

Rif ns Offerta.: 250827-01-A

FIDOGROUP
BV TECH

FIDOGROUP: INTRODUZIONE 4
OVERVIEW 5
AKAMAI CONNECTED CLOUD 5
FEATURE PRINCIPALI DI AKAMAI CONNECTED CLOUD 5
L'ARCHITETTURA GLOBALE DELLA PIATTAFORMA....7
L'EVOLUZIONE DI AKAMAI: CONNECTED CLOUD 8
IL PORTFOLIO DELLE SOLUZIONI AKAMAI.... 9
SECURITY & COMPLIANCE 11
APP & API PROTECTOR 11
OVERVIEW ARCHITETTURALE 11
PRINCIPALI FEATURES 13
CERTIFICATE PROVISIONING SYSTEM 14
SECURITY CONFIGURATIONS 15
LA POTENZA DEL MODELLO DI SECURITY ADATTIVO 15
LEADING ATTACK DETECTION 16
SECURITY TOOL COMPLETO E FACILE DA UTILIZZARE 17
AKAMAI BOT MANAGER 19
BOT MANAGER AI FRAMEWORK 19
MACHINE LEARNING AND THREAT INTELLIGENCE 20
BOT SCORING 20
OPZIONI DI CHALLENGE 20
VANTAGGI DELLA PROTEZIONE DEI GRANDI CLIENTI 20
KEY CAPABILITIES 21

FIDOGROUP
BV'TECH

CONSOLE DI GESTIONE: AKAMAI CONTROL CENTER ……21

PIANO DI IMPLEMENTAZIONE ……..24

ASSESSMENT ……24

DELIVERY ……..25

SUPPORTO NECESSARIO LATO CLIENTE ……26

FIDOGROUP
BV TECH

Fidogroup: Introduzione

Grazie ad anni di consolidata esperienza, Fidogroup fornisce una gamma di servizi professionali, tra cui l'installazione, il monitoraggio e l'analisi dei prodotti Akamai, per i quali detiene uno status di partnership Elite a livello europeo. In questo modo, Fidogroup garantisce la massima sicurezza ed efficienza dei sistemi informativi dei suoi clienti.

Il ruolo di Fidogroup come fornitore in questo contesto è altamente significativo e comprende diversi aspetti chiave:

Installazione dei prodotti Akamai: Fidogroup svolge un ruolo cruciale nell'installazione delle soluzioni Akamai per i suoi clienti. Questo processo garantisce che le piattaforme siano configurate correttamente e pronte per un uso efficace. Una corretta installazione è fondamentale per garantire la sicurezza e l'efficienza dei sistemi informativi dei clienti.

Monitoraggio dei prodotti Akamai: Fidogroup offre servizi di monitoraggio continuo per i prodotti Akamai. Ciò significa che le operazioni del sistema vengono monitorate proattivamente e qualsiasi anomalia o eventuale problema viene identificato tempestivamente. Il monitoraggio continuo aiuta a garantire che i sistemi rimangano operativi e sicuri nel tempo.

Analisi dei prodotti Akamai: Fidogroup conduce analisi approfondite sui dati provenienti dai sistemi di logging. Queste analisi possono aiutare a identificare tendenze, vulnerabilità o aree in cui è possibile un'ulteriore ottimizzazione del sistema. Questa analisi continua è importantissima per migliorare la sicurezza e l'efficienza delle infrastrutture esposte e protette.

Elite partnership status: Lo status di Fidogroup come partner Elite di Akamai a livello europeo sottolinea la competenza e stretta collaborazione con Akamai. Questo status infonde ulteriore fiducia nei clienti a cui Fidogroup può fornire servizi di alta qualità e la massima conoscenza dei prodotti.

In sintesi, Fidogroup svolge un ruolo cruciale nel garantire che i clienti siano dotati della migliore posture di security attraverso l'installazione, il monitoraggio e l'analisi dei prodotti Akamai, sfruttando la leadership di mercato in diversi settori e la partnership alla base di tutti i servizi.

FIDOGROUP
BV TECH

Overview

Akamai App & API Protector (AAP) combina web application firewall, mitigazione dei bot, sicurezza API e protezione DDoS di livello 7 in un'unica soluzione. Identifica rapidamente le vulnerabilità e mitiga le minacce su tutto il web e gli ecosistemi API del Cliente, anche per le architetture distribuite più complesse. Riconosciuto come la soluzione leader sul mercato per il rilevamento degli attacchi, **App & API Protector** è facile da implementare e utilizzare; fornisce aggiornamenti automatici per le protezioni di sicurezza e offre una visione olistica del traffico e degli attacchi.

Akamai Bot Manager (BM) complementa AAP e si concentra sul traffico bot più elusivo: utilizza tecnologie brevettate con un framework di intelligenza artificiale che analizza il traffico ai margini — dove un utente si connette per la prima volta a un'applicazione — fornendo dati puliti su modelli di traffico, tipologie e volumi per addestrare gli algoritmi di apprendimento automatico a essere più precisi. BM poi mitiga i bot dannosi ai margini, gestendo efficacemente anche i bot legittimi.
Sia AAP che BM forniscono ai clienti una vasta gamma di strumenti di visualizzazione e reportistica, oltre a opzioni di integrazione per DevSecOps.

Akamai Connected Cloud

Akamai AAP e BM sono costruiti sulla piattaforma "**Akamai Connected Cloud**", che costituisce la spina dorsale dell'infrastruttura di Akamai. Questa integrazione offre diversi vantaggi chiave in termini di prestazioni e scalabilità.

Feature principali di Akamai Connected Cloud

- Oltre 360.000 edge servers
- Più di 4.100 punti di presenza
- Oltre 1.200 ISP / operatori di rete mobile
- Presenza in tutti i 7 continenti
- 135 paesi, inclusa la Cina
- Più del 90% degli utenti Internet sono a un "hop di rete" da un server edge di Akamai
- Fino al 30% del traffico Internet giornaliero mondiale viene consegnato da Akamai
- Akamai consegna traffico web giornaliero raggiungendo picchi di oltre 275 Tbps
- SLA con uptime del 100%
- Caching avanzato, incluso il caching completo delle pagine
- Piattaforme separate di staging e produzione per i test delle implementazioni
- Il team di threat intelligence di Akamai analizza oltre 750 TB di nuovi dati di attacco ogni giorno

Akamai Connected Cloud è la più grande e affidabile piattaforma cloud ed edge del mondo. La massiccia distribuzione e integrazione nella quasi totalità della rete globale di Internet, insieme agli algoritmi più avanzati del mondo, sono dati fondamentali a dimostrazione della leadership di mercato – e solo Akamai decide dove e come instradare qualsiasi tipo di digital experience basandosi sulle reali prestazioni di Internet in ogni dato momento.

Akamai interagisce con miliardi di dispositivi client al giorno, assorbendo exabyte di dati all'anno, e li raccoglie in un data lake di oltre 7 petabyte per alimentare i motori di machine learning.
Grazie a questa enorme quantità di dati utente che mostrano come l'esperienza web stia effettivamente funzionando in tempo reale, l'intelligenza del **machine learning** di Akamai può identificare e mitigare le minacce alla sicurezza e i problemi nel percorso di delivery anche prima che diventino un problema per gli utenti. La scala massiccia e la distribuzione della piattaforma Akamai la rendono praticamente immune ai degradi della connettività e ai picchi di traffico che possono paralizzare altre piattaforme.
Quando si tratta di sicurezza, la scalabilità enorme della piattaforma Akamai consente di assorbire e mitigare anche i più grandi attacchi con un impatto minimo o inesistente sulle prestazioni delle applicazioni ed API.

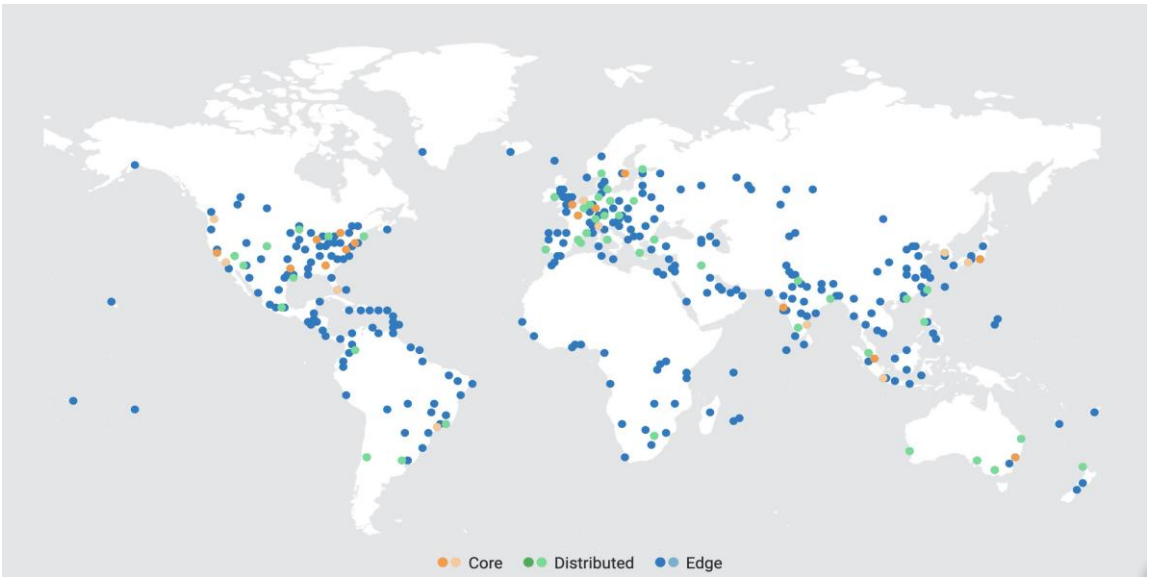
Gli attributi chiave di Akamai sono:

- **Uptime SLA del 100%**: applicazioni ed API funzionano perfettamente, ogni volta
- **Prestazioni consistenti**: capacità, distribuzione e scala per essere al top delle prestazioni su Internet con affidabilità del 100%
- **Accelerazione e routing intelligente**: i contenuti vengono memorizzati nella cache dell'infrastruttura edge e compressi come richiesto, e il traffico viene essere instradato in base a percorsi ottimizzati dinamicamente (sureroute) in tempo reale per essere accelerati al massimo
- **Modello di sicurezza basato sul cloud**: la sicurezza su Akamai è nativa in cloud, multilayer, pervasiva, portabile e indipendente dai perimetri di rete tradizionali
- **Integrità**: applicazioni ed API non hanno alcuna regressione e vengono servite esattamente nel modo in cui gli sviluppatori le concepiscono, indipendentemente da quanto siano estese, complesse o distribuite globalmente

L'architettura globale della piattaforma

Grazie alla sua architettura decentralizzata e all'ampia distribuzione in più di 130 paesi, Akamai è la piattaforma migliore per supportare clienti importanti come il Cliente. Grazie alla sua portata e presenza globale nelle reti ISP (più di 1200), la CDN garantisce prestazioni massime per il delivery dei contenuti.

La decentralizzazione e la distribuzione della piattaforma Akamai svolgono un ruolo chiave nel garantire ai Clienti uno SLA di disponibilità del 100%, grazie a più di **360.000 server edge** situati in oltre **4.100 POP**. Questo rende Akamai la piattaforma più distribuita al mondo in assoluto.



Grazie alla sua architettura, Akamai ha recentemente registrato diversi picchi di traffico sulla sua piattaforma, raggiungendo **fino a 260 Tbps**[1]. Questi picchi derivano essenzialmente da eventi globali contemporanei, come download e aggiornamenti di software combinati con eventi sportivi di grande pubblico.

La piattaforma Akamai può essere vista come una grande rete privata che collega e riduce le distanze tra utenti e origin, garantendo massima velocità, sicurezza e affidabilità per l'intero business digitale.

Lista dei paesi con POP Akamai

Akamai mantiene una rete globale di server per erogare i servizi:

[1] Akamai Internet Station: https://www.akamai.com/internet-station

- Albania
- Angola
- Antarctica
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Bermuda
- Bolivia
- Botswana
- Brazil
- Brunei Darussalam
- Bulgaria
- Cambodia, Kingdom of
- Canada
- Chile
- Christmas Island
- Colombia
- Costa Rica
- Croatia
- Curacao
- Cyprus
- Czech Republic
- Denmark
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Estonia
- Faroe Islands
- Fiji
- Finland
- France
- French Guyana
- Georgia
- Germany
- Ghana
- Gibraltar
- Great Britain
- Greece
- Greenland
- Grenada
- Guadeloupe (French)
- Guam (USA)
- Guatemala
- Guernsey
- Guinea
- Haiti
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kuwait
- Laos
- Latvia
- Lebanon
- Lesotho
- Lithuania
- Luxembourg
- Macau
- Macedonia
- Madagascar
- Malawi
- Malaysia
- Maldives
- Malta
- Martinique (French)
- Mauritius
- Mexico
- Moldova
- Monaco
- Mongolia
- Morocco
- Mozambique
- Myanmar
- Namibia
- Nepal
- Netherlands
- New Caledonia (French)
- New Zealand
- Nicaragua
- Nigeria
- Northern Mariana Islands
- Norway
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Qatar
- Reunion (French)
- Romania
- Russian Federation
- Rwanda
- Saint Lucia
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Singapore
- Sint Maarten
- Slovak Republic
- Slovenia
- South Africa
- South Korea
- Spain
- Sri Lanka
- Sweden
- Switzerland
- Taiwan
- Tanzania
- Thailand
- Trinidad and Tobago
- Tunisia
- Turkey
- Uganda
- Ukraine
- United Arab Emirates
- United States of America
- Uruguay
- Vanuatu
- Venezuela
- Vietnam
- Zamb

L'evoluzione di Akamai: Connected Cloud

Con l'annuncio di Febbraio 2023 riguardo Connected Cloud, l'offerta di Akamai sta adottando un approccio diverso al Cloud e integrerà siti di core compute distribuito in modo capillare. Akamai Connected Cloud è una piattaforma edge e cloud

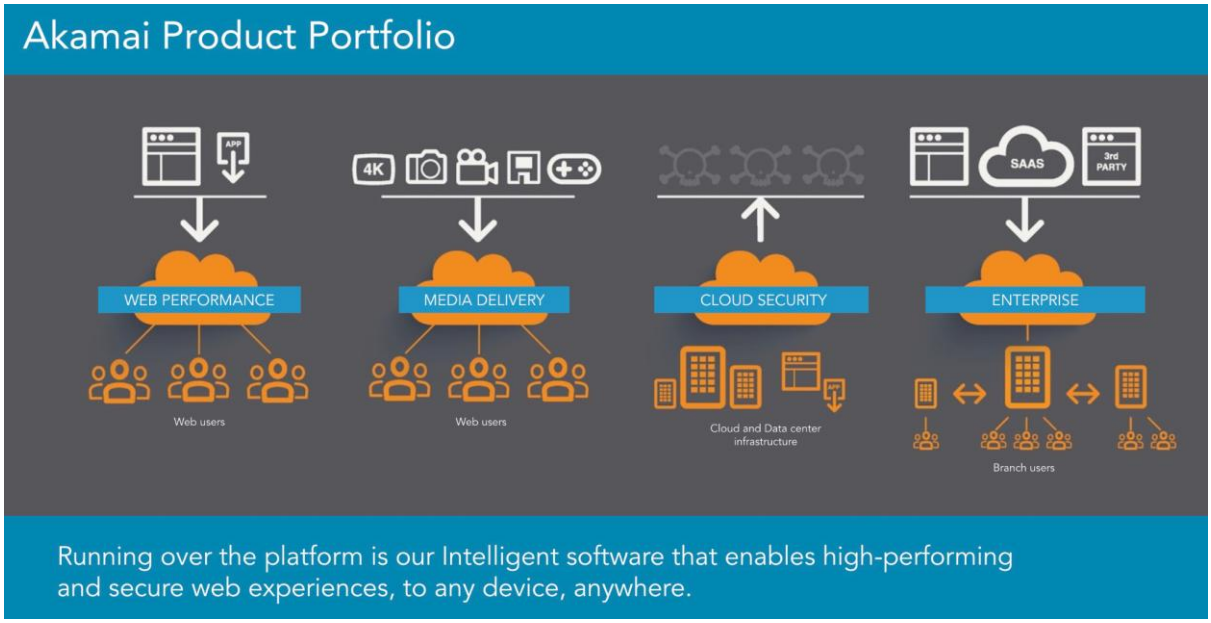
estremamente distribuita per il cloud computing, la security e il delivery di contenuti che avvicina le applicazioni agli utenti e allontana le minacce.

Con la creazione di Akamai Connected Cloud, Akamai sta aggiungendo siti core e distribuiti sulla stessa infrastruttura di base che oggi supporta la edge network. Più specificamente, Akamai sta avvicinando agli utenti, alle imprese e ai centri IT servizi di computing, storage, database e altre infrastrutture.
Il risultato mira a garantire una continuità del computing, dal core all'edge, consentendo alle aziende di creare, distribuire e proteggere in modo più efficiente workloads ad alte prestazioni che richiedono una latenza di solo pochi millisecondi e una portata globale.

Il Portfolio delle soluzioni Akamai2

Oltre all'offerta di computing risultante dalla sua più recente acquisizione, Akamai offre una vasta gamma di soluzioni tecnologiche che aiutano le aziende a fornire contenuti e servizi online in modo affidabile, sicuro e rapido. Il portfolio Akamai include quattro aree principali di soluzioni: **web acceleration**, **media delivery**, **cloud security** ed **enterprise security**.

[2] Saranno da considerare inclusi solo i prodotti menzionati esplicitamente nell'offerta



La **web acceleration** di Akamai aiuta a migliorare la velocità e l'affidabilità delle applicazioni web e delle API di un'azienda. Questo si traduce in una migliore esperienza utente e maggiore fedeltà del cliente. Akamai offre una gamma di soluzioni che includono la gestione del traffico web, l'ottimizzazione di immagini e video, la compressione dei dati il caching avanzato per ridurre i tempi di caricamento delle pagine.

Il **media delivery** aiuta a fornire contenuti video e audio in streaming a un vasto pubblico in modo rapido e affidabile. Akamai offre una gamma di soluzioni che includono la distribuzione di contenuti in streaming, la trasmissione di eventi dal vivo, la distribuzione di contenuti su dispositivi mobili e la monetizzazione degli stessi.

La **cloud security** aiuta a proteggere i servizi esposti dei clienti da una vasta gamma di minacce online: da attacchi DDoS, attacchi alle applicazioni, frodi sui browser, credential stuffing, brand impersonation, attacchi DNS, sicurezza delle API, ecc.

I prodotti di **enterprise security** consentono infine ai clienti di implementare un approccio Zero Trust o SASE nella protezione dell'azienda (dati sensibili, infrastruttura, flussi di dati e utenti interni).

In sintesi, Akamai è un'azienda che offre una vasta gamma di soluzioni tecnologiche per migliorare la velocità, l'affidabilità, la sicurezza e la flessibilità delle operazioni online delle aziende.

Security & Compliance

I servizi Akamai sono progettati per rispettare i requisiti GDPR in ogni norma e caratteristica. Le attività di trattamento dei dati condotte da Akamai tramite la nostra piattaforma di servizi sono svolte in modo da rispettare tutte le normative. Akamai viene anche valutata annualmente per la conformità con i seguenti standard:

Global	Regional
• PCI DSS • SOC 2 • ISO 27001 • ISO 27017 • ISO 27018 • ISO 27701	• FedRAMP • HIPAA • Cyber Essentials • BSI • IRAP • PSD2 • MAS

Per maggiori informazioni sulla compliance:
https://www.akamai.com/legal/compliance

APP & API Protector

Akamai **App & API Protector** è una soluzione omnicomprensiva che unisce molte tecnologie di sicurezza tra cui firewall per applicazioni web, mitigazione dei bot, sicurezza delle API e protezione DDoS.
App & API Protector è riconosciuto come la soluzione leader nella rilevazione degli attacchi, identificando e mitigando rapidamente le minacce al di là dei firewall tradizionali per proteggere interi patrimoni digitali da attacchi multidimensionali. La piattaforma è facile da implementare e utilizzare, offre una visibilità olistica e implementa automaticamente protezioni aggiornate e personalizzate tramite Akamai **Adaptive Security Engine (ASE)**.

Overview Architetturale

AAP è un Web Application Firewall in cloud (WAF) che garantisce l'integrità e la funzionalità di siti web, API e applicazioni web esposte su Internet e basate sui protocolli HTTP e HTTPS. È distribuito sulla Akamai Intelligent Edge Platform, composta da oltre **360.000 server** distribuiti in **135 paesi** e in grado di gestire picchi di **oltre 275 Tbps**.

Tutto ciò senza impattare sulle prestazioni: grazie ai protocolli ottimizzati, alle funzionalità di performance e all'offload che vengono garantiti rispetto all'origin, l'esperienza degli utenti finali migliora e viene accelerata oltre che diventare più sicura.
Infatti, i servizi Akamai AAP (e BM) includono funzionalità di Performance e Delivery, consentendo di scalare in modo fluido e automatico per adeguarsi alle richieste di traffico che variano nel tempo, distribuire risorse di CPU e memoria secondo necessità, consegnare contenuti memorizzati nella cache dall'edge e fornire una protezione continua senza interruzioni per il massimo livello di prestazioni sul delivery.

In particolare, per quanto riguarda la memorizzazione nella cache, la presente proposta include la possibilità di definire **regole di caching avanzate**, con **alta granularità** e **autoconfigurabili** sia tramite interfaccia web che tramite API.
I parametri delle regole includono: estensione del file, percorso, hostname, regex sul percorso del file, cookie, stringa di query e caratteristiche del dispositivo.
È possibile applicare una regola di caching no-store su tutte o su un sottoinsieme delle risorse da servire, così come definire regole diverse (non solo per scopi di caching ma per qualsiasi caratteristica applicativa, abbracciando così l'applicazione originale).
La memorizzazione nella cache include più livelli gerarchici di cache e funzionalità di accelerazione in caso di contenuto non disponibile o altri errori di delivery.

Gli attacchi volumetrici dell'ordine di anche **migliaia di Gbps** vengono assorbiti senza alcun impatto per il Cliente, grazie alla capacità di gestione del traffico in modo distribuito e alla capacità di calcolo disponibile.
I singoli domini (**FQDN**) possono essere presi in carico sul WAF di Akamai tramite una modifica al record DNS associato al servizio web da proteggere.
Per i servizi forniti tramite HTTPS, verranno generati sulla piattaforma Akamai dei certificati TLS dedicati, emessi a nome dell'azienda scelta.
Tutte le comunicazioni, sia da client ad Akamai che da Akamai all'origine, sono protette dal protocollo TLS con certificati validi firmati da Authority riconosciute (di default viene utilizzata Digicert per OV/EV e Letsencrypt per DV ma è anche possibile utilizzare certificati di terze parti), al fine di evitare attacchi man-in-the-middle e intercettazioni.
Questa modalità di funzionamento è progettata per gestire efficacemente la capacità di terminazione TSL di AAP (e BM), grazie alla quale possiamo raggiungere la postura di sicurezza ottimale contro un ampio spettro di minacce informatiche.
La piattaforma Akamai è conforme **PCI DSS Livello 3**.
Gli attacchi di livello 3/4 (come **UDP flood** o **SYN flood**) vengono semplicemente assorbiti dalla piattaforma scartando i pacchetti che non riescono a generare richieste HTTP complete.

Questa protezione integrata è inline e sempre attiva.

Per la protezione delle applicazioni, AAP incorpora un modulo WAF basato su tecnologia proprietaria, che genera allarmi di sicurezza o blocca gli attacchi vicino alla fonte che li ha originati, prima che raggiungano l'infrastruttura del Cliente.

Principali Features

AAP include un insieme completo di protezioni contro gli attacchi DoS e DDoS:

- **Protezione di livello 3/4 per attacchi DDoS** (UDP / SYN flood, fragmentation, reflection attacks, ecc.): grazie alla capacità della piattaforma di ricevere ed elaborare il traffico, questi attacchi vengono contrastati semplicemente scartando tutti i pacchetti di rete che non arrivano sulle porte TCP 80 (HTTP) o 443 (HTTPS) e non completano una richiesta HTTP correttamente formata.

- **Firewall Edge di rete (IP/Geo)**: i controlli IP/Geo bloccano o consentono il traffico proveniente da un IP specifico, da una sottorete, da un'area geografica o da un AS number. Questo permette di bloccare richieste malevole da indirizzi IP specifici o traffico da TOR, che gli hacker spesso utilizzano per nascondere la loro identità.

- **Protezione di livello 7 per attacchi DDoS** (GET / POST flood, ecc.): questi attacchi raggiungono la Piattaforma Akamai e vengono bloccati attraverso politiche di caching flessibili per risorse statiche e attraverso il "rate limiting" alle richieste di contenuto prima di inoltrarle all'origin. È possibile impostare vari tipi di rate limiting in modo granulare.

- **Protezione da attacchi “slow”** che mirano a esaurire le connessioni di un server: vengono gestiti bufferizzando le richieste in arrivo e impostando limiti di tempo per la ricezione della richiesta.

- **Protezione di livello 7 per attacchi alle applicazioni** (come SQL e command injection): questi attacchi vengono mitigati dal firewall WAF di Akamai, che sfrutta l'Adaptive Security Engine.

Tutti i vari strati di difesa inclusi in AAP sono rappresentati nell'immagine qui sotto:

Certificate Provisioning System

Il Sistema di Provisioning dei Certificati di Akamai (**CPS**) consente di auto-rilasciare e gestire i certificati TLS così come la configurazione delle opzioni TLS; tutte le opzioni possono essere gestite sia trmaite le API che il portale **Akamai Control Center** (ACC). Il CPS di Akamai offre una gestione completa del ciclo di vita dei certificati, con le seguenti opzioni:

- acquistare certificati di qualsiasi tipo per conto dei Clienti o self-provisioning
- aggiungere/rimuovere nomi host su certificati esistenti
- seguire il processo di rinnovo automatizzato o manuale
- definire le caratteristiche di rilascio (inclusi SNI, release programmata, approvazione della gestione dei change, staging e selezione delle cipher suites).

Grazie alla partnership con Autorità di Certificazione leader nel settore (Digicert e Letsencrypt), Akamai fornisce un portafoglio completo di opzioni di certificato:

- tutti i tipi di validazione dei certificati (**DV, OV, EV**)
- supporto per domini singoli e multipli (**SAN, SAN wildcard**); con supporto per tutte le diverse opzioni

- supporto certificati di terze parti per coprire casi aggiuntivi

Security Configurations

Una **security configuration** è il blocco di base che si utilizza per dividere ed impostare protezioni.
In ogni configurazione vengono definiti gli hostname inclusi ed una o più **security policy** associate, che consentono di impostare controlli per gestire diverse richieste (ad esempio, diversi set di protezioni per API e pagine web) e definire l'azione di risposta per ogni singolo item.
AAP include una ricca collezione di protezioni predefinite configurabili a livello di applicazione del firewall che vengono costantemente aggiornate dal gruppo di threat intelligence di Akamai.
AAP include anche l'opzione di definire **custom rules** per gestire scenari non coperti dalle regole standard e fornire la massima flessibilità.

L'interfaccia di configurazione delle **regole custom** consente di allertare o bloccare richieste in base a parametri come: metodo, percorso, estensione, header, cookie, query string, variabili del POST body ed altro.

Quando una hit attiva una regola WAF, le azioni di risposta possono essere configurate utilizzando parametri predefiniti, tra cui:

- Deny (bloccare la richiesta con una risposta 403 ed eventuale pagina di errore custom)
- Alert (loggare la richiesta)
- Inactive/Not Used (disabilitare il controllo)
- Abort (terminare la connessione senza inviare una risposta HTTP al client)

La personalizzazione della pagina di Deny si estende, oltre a poter definire un messaggio di errore riprendendo la grafica del portale e utilizzando la propria brand identity, anche di servire risposte XML, JSON o di qualsiasi altra tipologia.

La potenza del modello di security adattivo

Con App & API Protector, le protezioni di sicurezza vengono continuamente e automaticamente aggiornate con raccomandazioni di policy personalizzate implementabili con un solo click.
Adaptive Security Engine, la tecnologia alla base di App & API Protector, fornisce una protezione moderna combinando apprendimento automatico, security

intelligence in tempo reale, automazione avanzata e approfondimenti da oltre 400 ricercatori di threat esperti.

Adaptive Security Engine è unico sul mercato perché:

- Analizza le caratteristiche di ogni richiesta in tempo reale sulla rete Edge per una rilevazione più rapida ed efficace
- Impara i modelli di attacco sfruttando sia i dati locali che globali per apportare regolazioni di protezione specifiche per il cliente
- Si adatta alle minacce future, garantendo protezioni aggiornate anche con l'evolversi degli attacchi

Adaptive Security Engine allevia il carico di una sintonizzazione manuale e dispendiosa in termini di tempo con aggiornamenti automatici per un'esperienza quasi senza intervento, migliorando le rilevazioni di 2 volte e riducendo i falsi positivi di 5 volte.

Leading Attack Detection

Man mano che l'ambiente digitale di ogni cliente cresce, devono aumentare anche la profondità e l'ampiezza delle protezioni.
Oltre agli aggiornamenti automatici e all'auto-regolazione adattiva che l'Adaptive Security Engine offre, App & API Protector fornisce sistemi di rilevazione leader nel settore riconosciuti dagli analisti per il distributed denial of service (DDoS), bot, malware e altri vettori di attacco.

Protezione DoS/DDoS — Riconosciuto come una soluzione DDoS leader nel mercato, App & API Protector elimina istantaneamente gli attacchi DDoS a livello di rete direttamente sull'edge proteggendo anche dai picchi di traffico di un attacco.

Bot mitigation visibility — Visibilità in tempo reale sul traffico dei bot con accesso alla vasta directory di Akamai di oltre 1.700 bot conosciuti. Questo consente di indagare problematiche di proiezioni analytics distorte, prevenire il sovraccarico dell'infrastruttura di origin e creare definizioni di bot personalizzate per consentire l'accesso a bot di terze parti e partner senza ostruzioni. Controlli di sicurezza dei bot più sofisticati sono disponibili con Akamai Bot Manager Premier, per proteggere contro credential stuffing, web scrapers, creazione di account in massa, manipolazione dell'inventario e altri attacchi su carte di credito/loyalty cards.

Protezione dal malware — Questo modulo aggiuntivo può scansionare i file prima che vengano caricati ai margini per rilevare e bloccare il malware dall'entrare nei sistemi aziendali del cliente con caricamenti di file malevoli.

Site Shield — Previene gli attaccanti dal bypassare le protezioni basate sul cloud per prendere di mira direttamente l'infrastruttura di origine.

Security tool completo e facile da utilizzare

Akamai è dedicata all'evoluzione della piattaforma, rendendola sempre più completa e facile da usare abilitando protezioni sempre più avanzate ed aumentando la produttività delle aziende e di tutti i loro team.

Dashboard, allarmi e strumenti di reporting — accesso a strumenti di telemetria dettagliata degli attacchi, analisi degli eventi di sicurezza, creazione di allarmi email in tempo reale utilizzando filtri statici e soglie, e sfruttamento degli strumenti di reporting sulla sicurezza web che monitorano e valutano continuamente l'efficacia delle protezioni.
Più in generale, Akamai fornisce un ampio set di strumenti per il monitoraggio interattivo, il reporting e l'alerting, al fine di fornire documenti azionabili con insight tecnici e di business.

- **Strumenti di reporting dei servizi nel portale ACC**, che forniscono metriche di dashboard per ogni prodotto e servizio: i grafici scaricabili forniscono una visibilità granulare e approfondita in incrementi di 5 minuti, con una profondità storica di 90 giorni
- **Billing Center**, che fornisce un'anteprima delle metriche mese per mese e durante un mese di fatturazione calcolando i valori di queste metriche ogni notte
- **Allarmi**, configurabili sia nel portale ACC che tramite API, che forniscono notifiche automatiche e in tempo reale e informano direttamente quando le soglie predefinite sono state superate.

Integrazione DevOps — Le attività di configurazione e monitoraggio di Akamai possono essere gestite tramite il portale Akamai Control Center (ACC) o in modo programmatico, sfruttando Akamai per DevOps, che è una raccolta di integrazioni, strumenti e plug-in che aiutano a connettere i prodotti ai flussi di lavoro di automazione. Ecco alcune delle cose che questi strumenti possono fare:

- Costruire le protezioni attraverso processi semplificati
- Testare e Proteggere siti e applicazioni
- Rilasciare configurazioni di delivery
- Effettuare deployment tramite automazione

- Monitorare le applicazioni per varie problematiche e contribuire alla loro rapida risoluzione

Questi strumenti includono un insieme completo di API, oltre all'integrazione di **Akamai CLI** e **Terraform**, i team di security e operations possono sfruttare una vasta gamma di API di gestione e l'interfaccia a riga di comando (CLI) per integrare attività di configurazione di delivery e security nel processo CI/CD, abilitando le migliori pratiche di sicurezza nella progettazione.

Integrazioni SIEM — Sono disponibili API dedicate per i SIEM, e connettori preconfigurati per Splunk, QRadar, ArcSight ed altri sono automaticamente inclusi in App & API Protector. Più in generale, forniamo diversi modi per integrare senza problemi i nostri log con qualsiasi sistema di terze parti.

- Gli incidenti e gli eventi di sicurezza possono essere monitorati tramite il modulo di Integrazione **SIEM**, incluso nella presente proposta. Si basa su un'API completamente documentata, così come alcuni pacchetti preconfigurati per i sistemi SIEM più popolari
- I log completi HTTP(S) possono essere ricevuti in tempo reale con il modulo incluso di **DataStream**, che consente al Cliente di misurare la salute delle sue prestazioni, indagare su problemi di sicurezza e operativi, e visualizzare i dati con Datadog, Sumo Logic e BigQuery e tanti altri strumenti di observability e monitoraggio di log
- Ci sono anche API che consentono di ottenere statistiche sul traffico e di generare alert in caso di pattern di traffico inattesi. L'API Alerts consente di configurare notifiche su cambiamenti significativi del traffico basati sul monitoraggio continuo della piattaforma. Il sistema consente di creare e modificare allarmi basati su una vasta gamma di criteri, sia statici che dinamici, e di configurare report sulle anomalie
- Infine, l'**API Reporting** consente di generare vari report personalizzati con statistiche aggregate per aiutare a monitorare e ottimizzare i servizi

Altre feature incluse[3] — Per aumentare la visibilità e le prestazioni, App & API Protector ora include molti dei prodotti più apprezzati dai clienti, tra cui:

- **mPulse Lite** - Visibilità approfondita sul comportamento degli utenti, affronta i problemi di prestazioni in tempo reale e misura gli impatti su cambiamenti ed aggiornamenti
- **EdgeWorkers** - Serverless computing che consente di raggiungere scalabilità ancora maggiore con feature che aiutano a migliorare il time to market e l'esecuzione della logica sempre più vicino agli utenti finali
- **Image & Video Manager** - Ottimizza in modo intelligente sia le immagini che i video con la combinazione ideale di qualità, formato e dimensione

[3] Le offerte free tier hanno restrizioni sull'utilizzo

- **API Acceleration** - Migliora le prestazioni delle API gestendo facilmente l'accesso, scalando per picchi nei momenti di domanda e potenziando la sicurezza delle API

Akamai BOT Manager

Il Bot Manager di Akamai, con le sue capacità di rilevazione e mitigazione leader di mercato, consente di eseguire **operazioni automatizzate** in modo più efficace e sicuro, aumentando la fiducia dei clienti e dei loro interi ecosistemi.

La fiducia nel Bot Management di Akamai deriva dalla sua forza globale, sia tecnologica che come azienda. Akamai serve più del 50% delle organizzazioni globali 500 e ha oltre 4.100 punti di presenza in 135 paesi. Tutta questa forza è sfruttata per innovare continuamente il prodotto, garantendo che non si degradi nel tempo e rimanga all'avanguardia rispetto alle tendenze dei bot e alle tecniche di evasione.

Bot Manager utilizza molteplici tecnologie brevettate per rilevare e mitigare i bot nel punto in cui atterrano le richieste, piuttosto che permettere loro di raggiungere prima il sito di un cliente. La protezione è **costantemente aggiornata** man mano che le minacce si evolvono, con insights del team di threat intelligence sulle minacce incorporate automaticamente nei rilevamenti e nelle analisi del Bot Manager; i clienti non hanno bisogno di richiedere aggiornamenti speciali o miglioramenti in quanto la piattaforma si evolve costanemtente nel tempo in base al contesto di security attuale.

Bot Manager AI Framework

Il Framework AI del Bot Manager lavora inline sulla Akamai Intelligent Edge Platform. Questo consente al Bot Manager di osservare il traffico sull'edge, ovvero dove terminano le connessioni degli utenti, fornendo dati puliti sui modelli di traffico, i tipi di traffico e i volumi. In tutta la rete, Akamai vede in media 11,5 miliardi di richieste di bot al giorno e 280 milioni di accessi di bot.

Bot Manager impiega molteplici rilevamenti stratificati per identificare l'attività delle botnet, inclusi rilevamenti basati su signature, comportamentali e anomalie statistiche.
Approcci signature-less che sfruttano big data e machine learning distinguono l'attività dei bot più avanzata dall'uso legittimo. Le insight di **threat intelligence** vengono incorporate dai ricercatori costantemente ed automaticamente; una volta

rilevata una minaccia, BM mitiga gli attacchi dei bot con azioni configurabili che possono andare oltre il blocco e il permesso, servendo eventuali contenuti alternativi, challenge, rallentando le risposte e altro ancora.

Machine learning and threat intelligence

La raccolta di dati su "traffico pulito" su una vasta distribuzione di tipologia di dato e in grandi volumi addestra gli algoritmi di machine learning rendendoli sempre più accurati.
Questa visibilità dei dati consente agli algoritmi di imparare di più e più velocemente.
Il team di **threat hunting** di Akamai segue costantemente le tendenze nei modelli di attacco, nell'innovazione tecnologica e nuove evasioni per migliorare i rilevamenti.

Bot Scoring

Il bot score combina tutti i trigger di rilevamento per identificare bot sofisticati e fornire una valutazione più accurata di ogni richiesta, ottimizzando l'efficacia complessiva del rilevamento del sistema — il tutto senza aggiungere latenza e senza perdere prestazioni.

Opzioni di challenge

La combinazione della capacità di Bot Scoring con il sistema di challenge all'avanguardia fornisce la sicurezza di agire automaticamente utilizzando soglie predefinite e azioni di risposta. La **Crypto Challenge** costringe i bot a spendere cicli CPU in puzzle crittografici con un tempo minimo di risoluzione, rallentando gli attacchi dei bot sofisticati e aumentando i costi per gli aggressori. L'interstitial challenge richiede ai clienti di dimostrare che supportano il salvataggio dei cookie e l'esecuzione di JavaScript. In caso contrario, il sistema impone una penalità temporale più qualsiasi azione di risposta scelta come mitigazione.

Vantaggi della protezione dei grandi clienti

Alcune delle più grandi e rinomate aziende del mondo sono protette da bot manager e diventano spesso bersaglio dei più avanzati bot operators.
Se un nuovo bot viene rilevato presso un cliente, i dati sul bot vengono aggiunti alla libreria dei bot conosciuti e agli algoritmi per tutti i clienti.
Questo effetto non solo permette ai clienti di gestire efficacemente i bot, ma consente anche di fermare preventivamente alcuni bot dall'attaccare altri clienti.

Key Capabilities

Directory bot conosciuti — Bot Manager risponde automaticamente in modo adeguato ai bot conosciuti; l'attuale directory di 1.750 bot conosciuti è continuamente aggiornata.

Rilevamenti dinamici e sofisticati dei bot — Bot Manager rileva accuratamente i bot sconosciuti fin dal primo contatto utilizzando una varietà di modelli e tecniche di AI e machine learning.

Modello di punteggio — Il modello di Punteggio Bot valuta ogni richiesta con tutti i rilevamenti di Bot Manager Premier. Calcola poi la probabilità che la richiesta provenga da un bot e emette un punteggio da 0 (umano) a 100 (sicuramente un bot).

Impostazione personalizzata per endpoint — La capacità di Punteggio Bot consente di impostare risposte strategiche diverse per ogni endpoint.

Simulatore di risposte — Le risposte strategiche possono essere sintonizzate in base all'endpoint e alla tolleranza al rischio di un'organizzazione. Il Punteggio Bot consente di simulare la sintonizzazione prima che venga messa in atto — visualizzando l'impatto del cambiamento delle soglie basato sul traffico passato.

Autotuning — Bot Manager apprende i modelli di traffico normali di un sito (o siti) e sintonizza automaticamente i rilevamenti in base ai modelli unici per evitare richieste potenzialmente classificate erroneamente.

Nuanced response actions — La mitigazione dei bot è potenziata con azioni che vanno oltre il deny e l'allow, come servire contenuti alternativi, presentare challenge, rallentare le connessioni (tarpit) e altro ancora.

Reporting e analisi granulare — Le decisioni possono essere prese in base a dati affidabili con il reporting in tempo reale e storico di Bot Manager.

Console di Gestione: Akamai Control Center

Per controllare e gestire i servizi sopra descritti, sarà reso disponibile l’accesso al portale WEB denominato **Akamai Control Center.**
Questa rappresenta una **Console di Gestione** user friendly, che consentirà al Cliente di configurare i servizi Akamai attivati, di monitorarne le prestazioni, di effettuare analisi sul traffico gestito e sui servizi di sicurezza e di generare report.

Tra le caratteristiche di utilizzo sono previsti e confermati i seguenti punti:

- autenticazione in modalità multi-factor mediante l'utilizzo di password e token. La soluzione consente di definire specifiche regole per la costruzione di password complesse
- accessibilità mediante un protocollo sicuro, previa autenticazione, per mezzo dei più diffusi web browser
- interfaccia utente multi-lingua incluse italiano e inglese;
- context dedicato esclusivamente alle risorse del Cliente e prevede la possibilità di profilare gli utenti con un altissimo livello di granularità, definendo ruoli ad-hoc configurabili secondo accessi funzionali e di risorse inclusi i seguenti profili:
    - Amministratore: ha tutti i privilegi concessi, inclusa la possibilità di creare nuovi utenti
    - Configuratore: per modificare/aggiornare configurazioni e "rule set" (es. in caso di attacco in ambiente di produzione oppure per test in ambiente di pre-produzione)
    - Analista: operatore che ha visibilità su quanto necessario per monitorare lo stato di sicurezza complessivo delle varie risorse protette
- Integrazione con i sistemi di Single Sign-On del cliente

Il portale Akamai Control Center si compone dei seguenti principali moduli:

- Property Manager: consente di creare, modificare e distribuire le configurazioni dei servizi Akamai attivati; le modifiche inserite vengono abilitate in modo sicuro attraverso la rete globale Akamai mediamente entro 10 minuti
- Event Center: consente di gestire eventi relativi ai servizi Akamai attivati, diventando un supporto per la pianificazione, la gestione e la reportistica. Questo modulo è utilizzato in prevalenza per i servizi di delivery, più che per la gestione dei servizi di sicurezza come APP & Api Protector e Prolexic
- Resolve: offre informazioni di supporto in tempo reale per il corretto utilizzo del portale e per la gestione dei media per i servizi Akamai di accelerazione WEB.
- Reporting: offre funzionalità avanzate di reporting interattivo per avere una visibilità immediata sull'operatività dei servizi Akamai attivati e consentirne l'analisi approfondita. Oltre alle pagine di panoramica, è possibile generare grafici e reports per specifici intervalli di tempo o drill down sui dati visualizzati per ottenere maggiori dettagli.

Il portale Akamai Control Center consente inoltre di configurare funzioni di alerting adattivo per segnalare specifici eventi di sicurezza o discostamenti da un modello di traffico gestito predefinito, in modo tale da potere attivare anche proattivamente le misure di protezione necessarie. Gli alert saranno configurati e attivati nella fase di tuning del servizio.
Specificatamente per quanto riguarda il servizio WAF il portale mette a disposizione la sezione "Cloud Security Solutions - Security Center".

Il Security center consente di ottenere sia un overview generale delle configurazioni di security applicate, sia un monitoring costante dei flussi di traffico gestiti, differenziando il traffico standard dal traffico di attacco. Il modulo è in pratica una dashboard che visualizza informazioni di alto livello su eventi di sicurezza, traffico e attività di attacco che sono suddivise in quattro categorie:

- attacco DoS
- attacco a livello di applicazione
- attività BOT
- altre attività (che riflettono l'attività delle regole personalizzate).

Il **Security Center** fornisce i dettagli per un monitoring efficace e puntuale dello stato di sicurezza sulle applicazioni oggetto di protezione WAF:

- Chi (Who): Chi sta attaccando il sito (in base all'indirizzo IP, alla sessione e alla reputazione dell'attaccante)?
- Dove (Where): Da quale paese proviene l'attacco?
- Quando (When): Quando è iniziato l'attacco? Quando è finito l'attacco? (Tendenze generali di attacco e ricorrenza)
- Come (How):
    - Come è stato attaccato il sito (tipo di attacco, vettore di attacco)?
    - In che modo Akamai ha gestito l'attacco (quali regole e policy sono state attivate)?
    - Quanto è efficiente la configurazione di sicurezza adottata?
- Che cosa (What):
    - Quale sito era sotto attacco?
    - Qual è la copertura di sicurezza?
    - Cosa è disponibile in KSD che non sto utilizzando?
    - Quali nuove minacce stanno venendo fuori?
    - Qual è stata la risposta di Akamai all'attacco (alert / deny / other)?
    - Qual è stato l'impatto dell'attacco sul traffico generale?
    - Qual è stato l'impatto dell'attacco sulle prestazioni del sito?

Quindi dai reports resi disponibili potranno essere recuperate le seguenti informazioni:

- Numero di hit/s o Volume di traffico in Mb/s o page request per secondo.
- Policy di sicurezza applicate in risposta agli attacchi subiti o per specifica tipologia di attacco.
- Attacchi provenienti da un dato paese o regione geografica.
- Attacchi subiti su una specifica URL.
- IP sorgenti degli attacchi subiti, suddivisi anche per specifica tipologia di attacco.
- Statistiche sull'utilizzo delle black list configurate.

- Statistiche sull'applicazione delle policy di rate control e reputation control.

I reports hanno rappresentazione sia grafica che tabellare e nella maggior parte dei casi è possibile scaricarli anche in formato CSV.
Oltre ai reports standard il Security Center consente di creare reports personalizzati in base ai dati collezionati dalla piattaforma Akamai, sia a livello "Executive" che prettamente tecnico con dettagli su tutte le richieste.

Piano di implementazione

Il piano di implementazione della soluzione WAF, che comprende anche gli elementi di Bot Management e CDN, può essere diviso in milestones contenenti i loro deliverables e processi.

Assessment

La prima fase progettuale sarà quella di assessment, dove il team di Solution Architects di Fidogroup collaborerà con i team del Cliente (ed eventualmente tutte le entità che esso coinvolgerà nel progetto) per raccogliere lo scope esatto dell'attività con diversi meeting, il cui effort dipenderà dalla complessità intrinseca dell'infrastruttura e delle applicazioni da proteggere.

I meeting saranno utili a definire puntualmente tutti i dettagli necessari a proteggere efficacemente le risorse di Cliente, con la necessità di avere almeno una figura tecnica presente per ognuna delle seguenti aree:

- Infrastruttura IT - per poter descrivere la parte infrastrutturale, tipicamente lo stack web (load balancer / frontend / backend / database) e quello DNS
- Team Applicazioni - è cruciale comprendere il funzionamento delle applicazioni ad alto livello in modo da configurare le policy di delivery e di security
- Team di Security - è cruciale determinare come vengono attualmente messe in sicurezza le infrastrutture e le applicazioni verificando tutto lo stack e considerando la presenza di apparati come firewall, IDS/IPS, EDR/XDR o qualsiasi altro appliance software/hardware in grado di filtrare e gestire il traffico

La fase di assessment produrrà il primo **deliverable**: ovvero un documento che certificherà la perfetta compatibilità degli asset garantendo l'assenza di possibili regressioni nonché tutte le informazioni tecniche necessarie al team di Solution Engineers per un'efficace fase di delivery.
Il secondo deliverable sarà un il **piano di progetto** che dettaglierà ogni singola attività ed il tempo dedicato a completarla con gli effort e le risorse assegnate, collegando ogni task ai prerequisiti necessari.

Delivery

A seguito del completamento della fase di assessment si passa a quella di delivery, dove viene messo in opera il piano di progetto per portare avanti le attività di onboarding, con le macrofasi di configurazione, testing, go-live e tuning di delivery e security.

Il piano di delivery per un'applicazione o un gruppo di applicazioni conterrà una serie di attività che includono una breve descrizione, l'effort necessario e le risorse assegnate; le tempistiche potranno variare in base alla disponibilità del team di Cliente, il gruppo di Fidogroup potrà chiaramente garantire i tempi dichiarati nel progetto per le attività competenti.

Un esempio di piano di progetto che copre la stragrande maggioranza dei casi si struttura solitamente come segue:

- Preparazione degli asset Akamai
  - Richiesta Certificati
    - Richiesta CSR (1gg, Fidogroup)
    - Validazione Dominio (1gg, Fidogroup)
    - Validazione dell'Organizzazione (5gg, Cliente)
  - Creazione degli hostname di origin (2gg, Fidogroup)
  - Creazione e condivisione della mappa siteshield per limitare l'accesso firewall (2gg, Fidogroup)
- Preparazione dell'infrastruttura di origin
  - Provisioning dei certificati LB/Frontend (se necessario) (5gg, Cliente)
  - Definizione delle firewall policy (TBD, Cliente)
  - Disattivazione quarantente sulle appliance di security (TBD, Cliente)
- Configurazione su Akamai
  - Configurazione di delivery (10gg, Fidogroup)
  - Configurazione di security in alert mode (5gg, Fidogroup)
  - Testing funzionale (TBD, Cliente)
  - Approvazione delle configurazioni e schedulazione dei meeting per il go-live (1gg, Cliente)
- Attività di Go-Live
  - Switch degli hostname di produzione verso Akamai (1gg, Fidogroup/Cliente)
  - Testing (Fidogroup/Cliente)
  - Monitoraggio (Fidogroup)
- Learning Mode (10gg, Fidogroup)

- Attività di Deny Mode
  - Analisi del traffico ricevuto (15gg, Fidogroup)
  - Richiesta di change verso Cliente e discussione delle review (1gg, Fidogroup/Cliente)
  - Verifiche, testing e approvazione dei change (Cliente)
  - Switch in deny mode (2gg, Fidogroup)
  - Monitoraggio (2gg, Fidogroup)
- Blocco Siteshield
  - Collezione del traffico su origin (10gg, Cliente)
  - Analisi e conferma (2gg, Fidogroup)
  - Approvazione e commit delle policy firewall (1gg, Cliente)

Supporto necessario lato Cliente

Potrebbe essere necessario, seppur riducendo sempre al minimo l'effort e sempre con tutta l'assistenza e la supervisione dei tecnici Fidogroup, supporto per le seguenti attività, dipendentemente dalle necessità:

- Change sull'infrastruttura locale/Cloud, per poter controllare come l'origin interagisce con le tecnologie WAF/CDN
- Supporto del team applicativo per conoscere al meglio lo stack software e il funzionamento di applicazioni ed API
- Supporto del team di testing (ove presente) per portare avanti le attività di validazione di ogni configurazione ed assicurarsi un passaggio ad impatto zero, in alternativa sono utilizzabili piani di testing già definiti in caso il Cliente ne sia dotata
- Supporto del team di security per portare avanti change sui firewall ed altri apparati di sicurezza, escalation su incidenti e domande generali sull'integrazione con altre appliance e/o security practices da implementare lato Akamai
- Change mangement, anche se le attività lato Akamai vengono solitamente portate avanti senza impatti, sarà necessaria conferma per ogni change sul network di produzione, Fidogroup non porterà avanti nessun change se non dietro conferma scritta