FORTINET | COLOMBIA & ECUADOR

XPERTS26

Cuando la aplicación es la nueva frontera

Una sola Plataforma para proteger las aplicaciones

Disclaimer

Fortinet Confidential

This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Presentadores

Ana María Fuentes

Principal Systems Engineer

David Zambonino

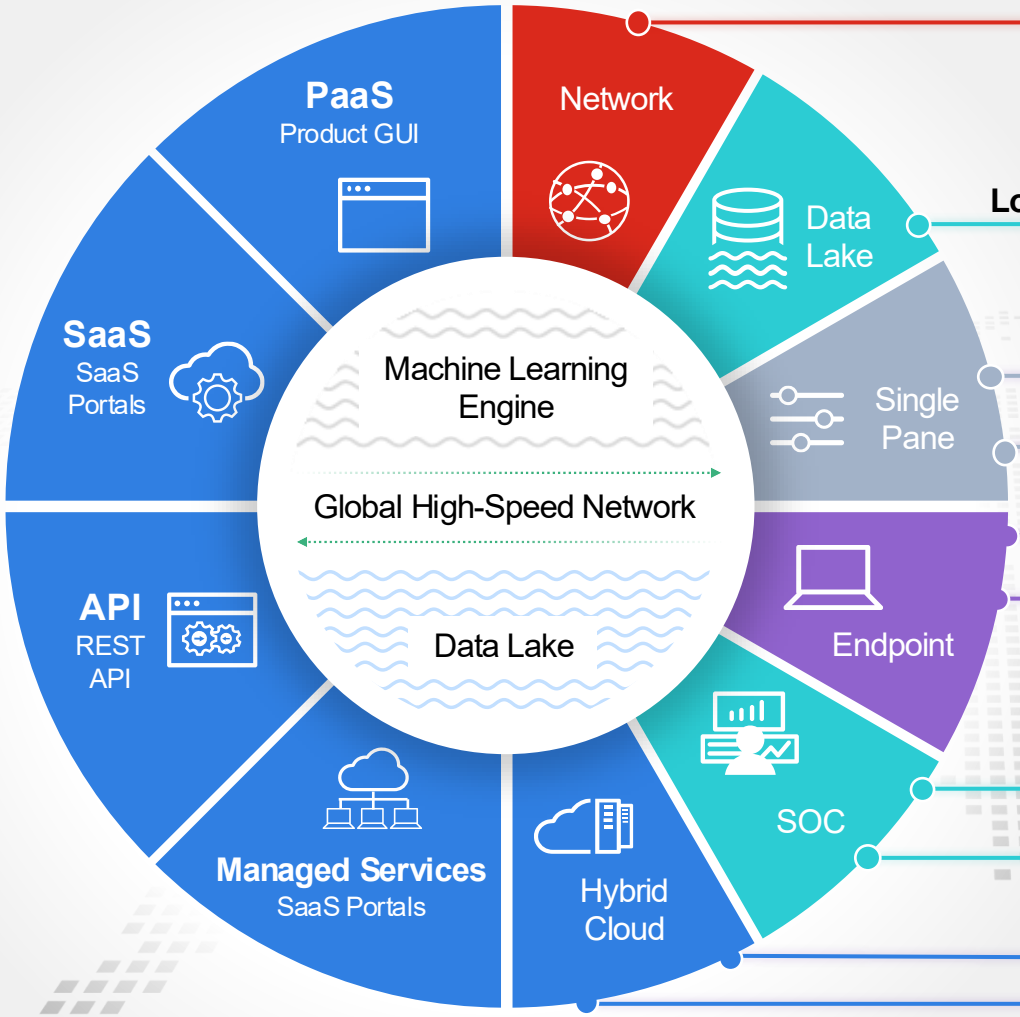
Cloud Subject Matter Expert - LATAM

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Bienvenidos a la era de la Plataforma

FortiCloud



What connects to FortiCloud?

Network Traffic

- SASE Endpoints
- Web Traffic (WAF)
- Thin Edges
- GSLB Users

Logs, Events & Long Term Data

- FortiGate
- FortiClient
- FortiEDR

Management

Alerts

- DCFW
- LAN
- Cloud FW
- NGFW
- WWAN
- DEM

Management

Events

- ZTNA / EPP
- MFA Tokens
- EDR / XDR

Content for Analysis

Events

- DCFW
- Mail
- NGFW
- Endpoint

Management

Logs

- Cloud Native FW
- Code Security
- SaaS (CASB)
- Oversight (CNAPP)

Ciberseguridad como Servicio

FortiFlex

- Licencias de uso flexibles, basadas en puntos, que simplifican los procesos de adquisición y los gastos operativos

Reduce el gasto comprometido y permite controlar los costos al ajustar el consumo de servicios al nivel adecuado. Los puntos no utilizados pueden transferirse anualmente al renovar el servicio.

Amplía o reduce las implementaciones sin demoras en la adquisición.

Independiente de la nube y de la plataforma en todas las implementaciones.

Visibilidad centralizada, administración de licencias y automatización basada en API.

aws Google Cloud ORACLE CLOUD

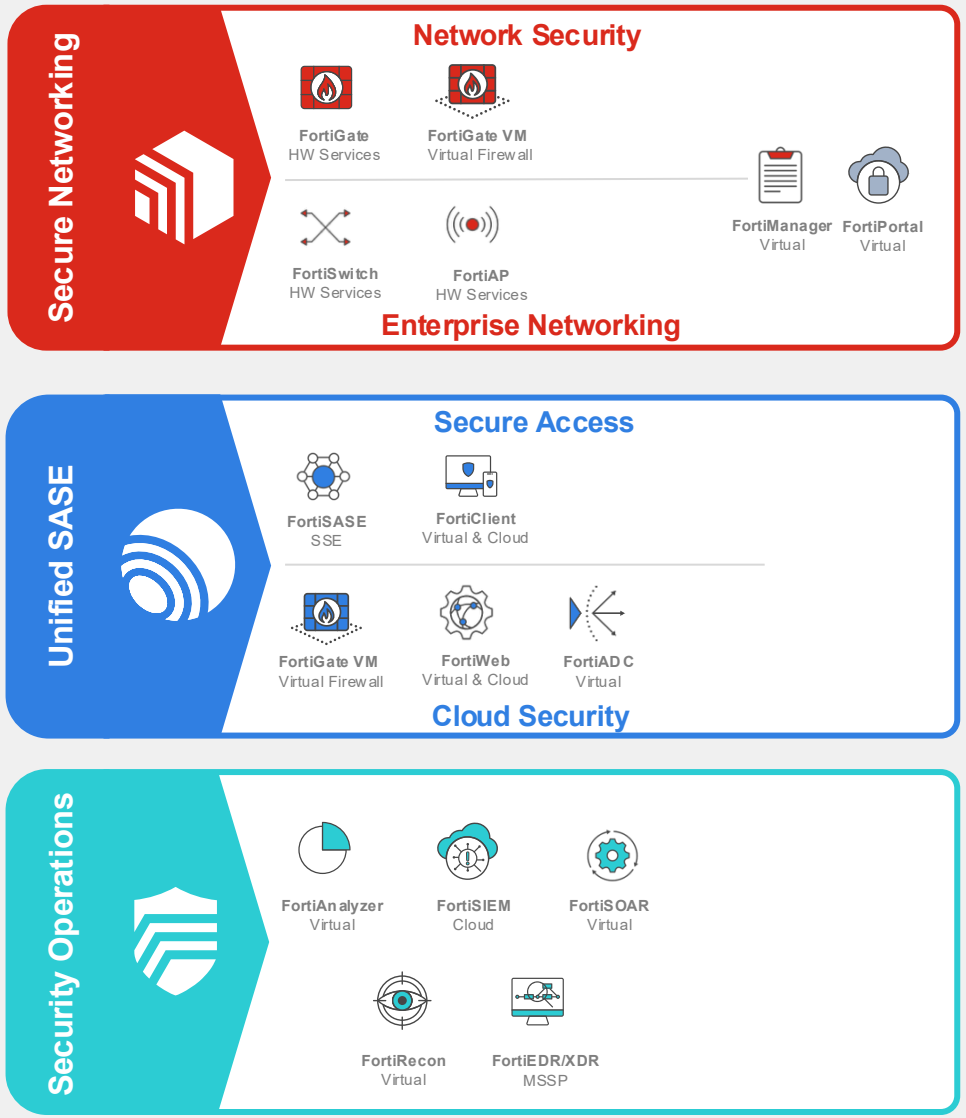
FortiFlex: Licencias basadas en el uso

FortiFlex Credits

- Agrega puntos en en cualquier momento
- Transfiere los puntos no utilizados a una suscripción válida*

Provision through FortiFlex portal or API

- Cualquier servicio de FortiGuard o FortiCare
- Cualquier tamaño o cantidad de máquinas virtuales
- Se puede implementar en las instalaciones o en la nube



Los clientes solo pagan por lo que usan a diario

* https://docs.fortinet.com/document/flex-vm/23.2.0/administration-guide/667344/points

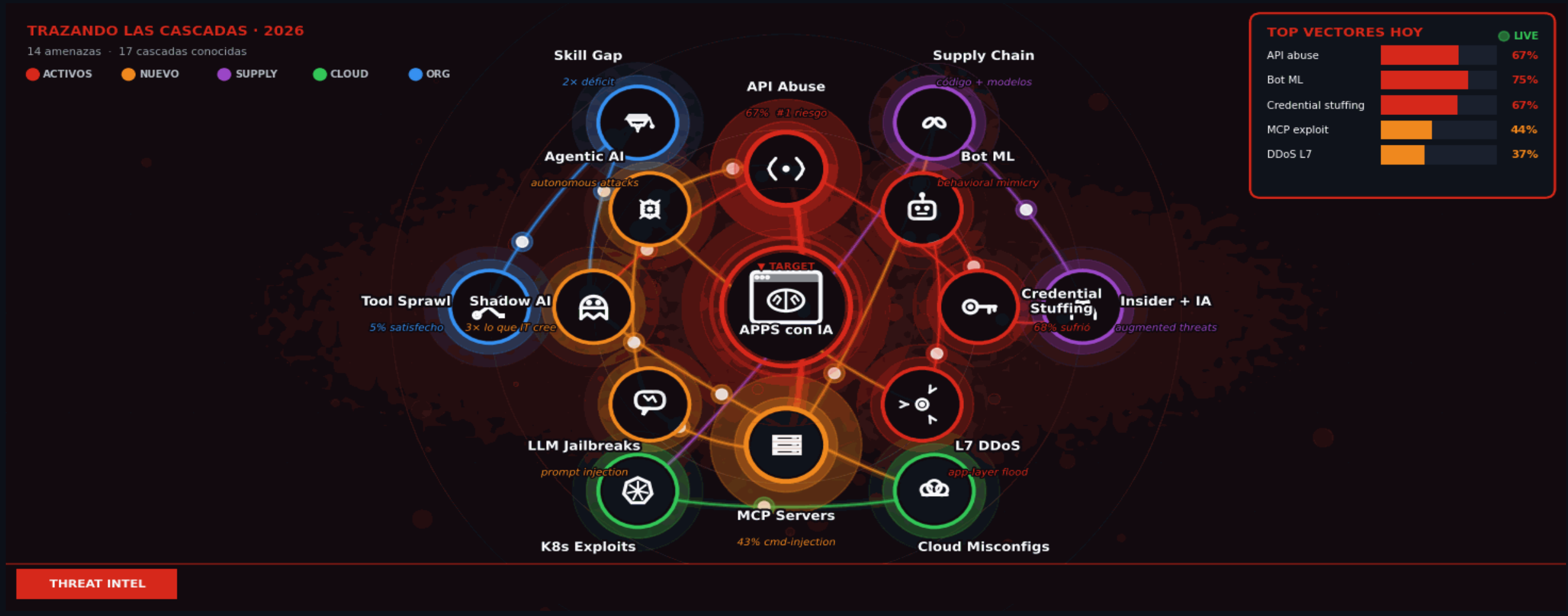
FORTINET | COLOMBIA & ECUADOR

XPERTS26

Contexto de aseguramiento de aplicaciones modernas

Panorama de amenazas AppSec 2026

No es una lista. Es una red. Una amenaza no llega sola — arrastra otras 5.



THREAT INTEL

Fuente: Fortinet Web AppSec Report 2026 · OWASP MCP Top 10 · Threat Intel FortiGuard

Riesgos latentes

A01

Broken Access Control

A02

Security Misconfiguration

A03

Supply Chain Failures

A04

Cryptographic Failures

A05

Injection

A06

Insecure Design

A07

Authentication Failures

A08

Data Integrity Failures

A09

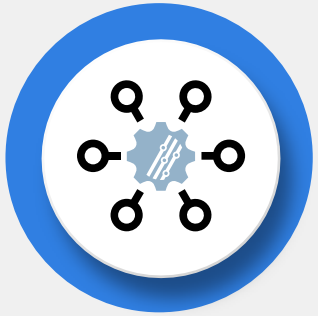
Logging & Alerting Failures

A10

Mishandled Exceptions

Objetivos del Cliente

Disponibilidad en todo momento



Rendimiento Optimizado

Máxima Seguridad

Ambientes listos multi-cloud e híbridos

Desafíos técnicos

1 Flexibilidad arquitectónica

Appliances → Híbrido Nube

2 Tecnologías de TI

Monolítico → Microservicios

3 Herramientas CI/CD

Manual → Automatización

4 Aumento de la superficie de ataque

Aplicaciones web → API, Archivos, Bots

EVOLUCIÓN DE TI Y DESARROLLO

De sistemas monolíticos a aplicaciones inteligentes, distribuidas y automatizadas

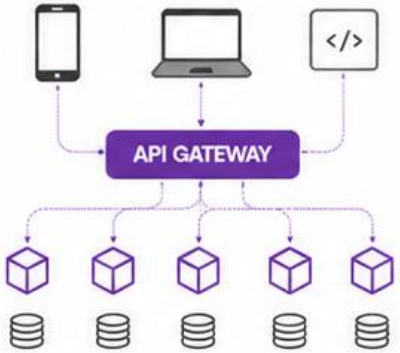
1 ERA MONOLÍTICA
1990s – 2000s

Aplicaciones monolíticas on-premise

- Aplicaciones web simples
- Arquitectura monolítica
- Infraestructura propia
- Despliegues manuales
- Equipos centralizados

2 ERA DE APIS Y MICROSERVICIOS
2000s – 2010s

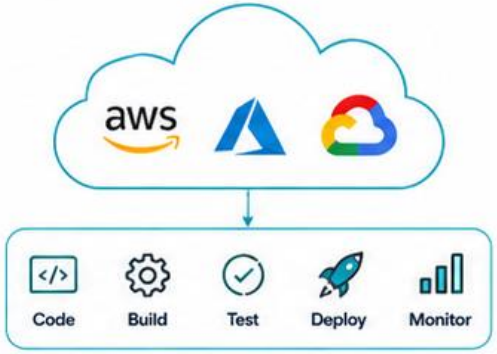
Arquitecturas orientadas a servicios y exposición de APIs



- SOA y servicios reutilizables
- Exposición y consumo de APIs
- Microservicios iniciales
- Equipos por capacidad / producto
- Mayor escalabilidad

3 ERA CLOUD & DEVOPS / CI/CD
2010s – 2020

Cloud, automatización y entrega continua



- Adopción de cloud (pública / híbrida)
- DevOps y cultura Ágil
- CI/CD y automatización
- Contenedores y orquestación (Docker, K8s)
- Infraestructura como código (IaC)
- Observabilidad y monitoreo continuo

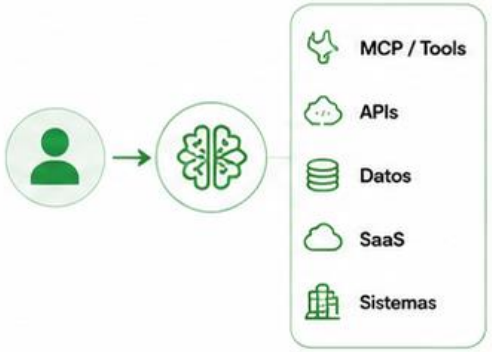
4 ERA MULTICLOUD & PLATAFORMAS
2020 – 2024

Plataformas cloud-native, serverless y event-driven

- Estrategias multicloud
- Cloud-native y serverless
- Arquitecturas event-driven y APIs
- Plataformas como servicio (PaaS)
- Datos distribuidos
- Seguridad y networking integrados

5 ERA AI-DRIVEN & APLICACIONES INTELIGENTES
2024+

IA, datos y automatización como motor de las aplicaciones



- IA generativa y agentes
- LLMs integrados en aplicaciones
- Automatización cognitiva
- MCP para acceso a herramientes y datos
- Experiencias hiper-personalizadas
- Decisiones basadas en datos e IA

EVOLUCIÓN DE UNA APLICACIÓN DE RETAIL

De una tienda web monolítica a una experiencia inteligente y personalizada

1 TIENDA WEB MONOLÍTICA

2000s

Experiencia web básica desde un solo sistema. Cambios lentos y alta dependencia del área de TI.

- On-premise
- Aplicación monolítica

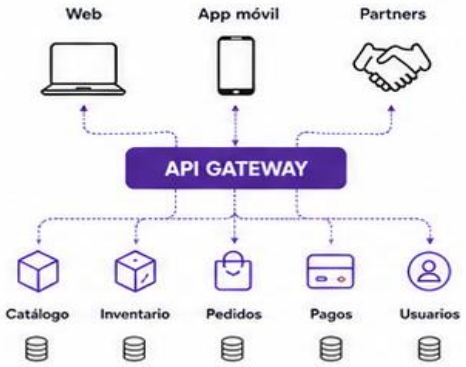
EXPERIENCIA HABILITADA

El cliente consulta el catálogo y compra desde la página web.

2 APIS Y MICROSERVICIOS OMNICANAL

2010s

Nuevos canales y servicios expuestos vía APIs. Catálogo, inventario, pedidos y pagos reutilizables en todos los canales y con terceros.



- Arquitectura de microservicios
- APIs reutilizables
- Integración con terceros

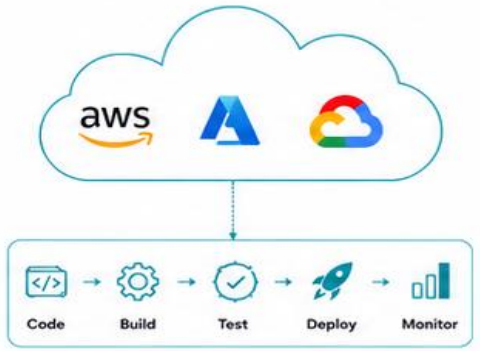
EXPERIENCIA HABILITADA

El cliente compra desde la app, consulta inventario de una tienda y selecciona retiro en tienda (click & collect).

3 ERA CLOUD & DEVOPS / CI/CD

2010s – 2020

Cloud, automatización y entrega continua para innovar más rápido y escalar automáticamente ante picos de demanda.



- Adopción cloud (pública / híbrida)
- CI/CD y automatización
- Observabilidad monitoreo

EXPERIENCIA HABILITADA

El retailer lanza una promoción de Black Friday rápidamente y escala la plataforma ante el aumento de transacciones.

4 ECOSISTEMA DIGITAL MULTICLOUD

2020s

Plataforma conectada con múltiples servicios y partners para ofrecer una experiencia completa y operar a escala global.

- Arquitectura distribuida y multicloud
- Integración con SaaS y partners
- Alta disponibilidad y escalabilidad

EXPERIENCIA HABILITADA

Una compra coordina en tiempo real inventario, pago, operador logístico, marketplace y comunicaciones al cliente (email, WhatsApp).

5 AI-DRIVEN APPLICATION SHOPPING ASSISTANT

2024+

IA, datos y automatización como motor de la experiencia. Agentes inteligentes entienden la intención del cliente y ejecutan acciones con herramientas del negocio.

- IA generativa y agentes
- Automatización cognitiva
- Experiencias hiper-personalizadas

EXPERIENCIA HABILITADA

El cliente expresa lo que necesita y un asistente de IA consulta productos, precios e inventario para ayudarlo a completar la compra.

EVOLUCIÓN DE UNA APLICACIÓN PETROTÉCNICA

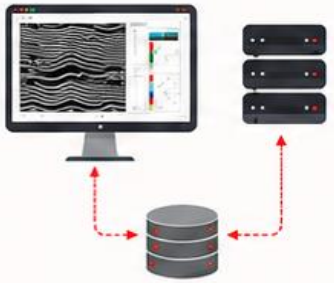
De una aplicación monolítica de análisis del subsuelo a una plataforma inteligente con IA

1 APLICACIÓN MONOLÍTICA

Una única aplicación instalada on-premise concentra todas las funcionalidades y datos.

ARQUITECTURA

Aplicación monolítica



Almacenamiento local (servidores y storage) en el data center de la empresa.

EJEMPLO

Un analista revisa manualmente imágenes sísmicas y datos de pozos desde la aplicación instalada en su estación de trabajo.

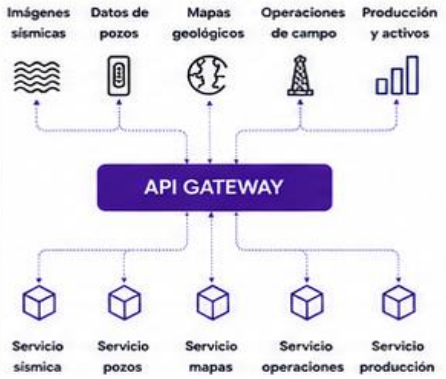
IMPACTO AL NEGOCIO

Procesamiento lento y limitado, dependencia del hardware local y colaboración restringida.

2 APIS Y MICROSERVICIOS

La aplicación se descompone en servicios más pequeños y se expone mediante APIs para integrarse con otros sistemas.

ARQUITECTURA



EJEMPLO:

La información de sísmica, pozos y operaciones se comparte mediante APIs con otras aplicaciones como perforación, reservorios y producción.

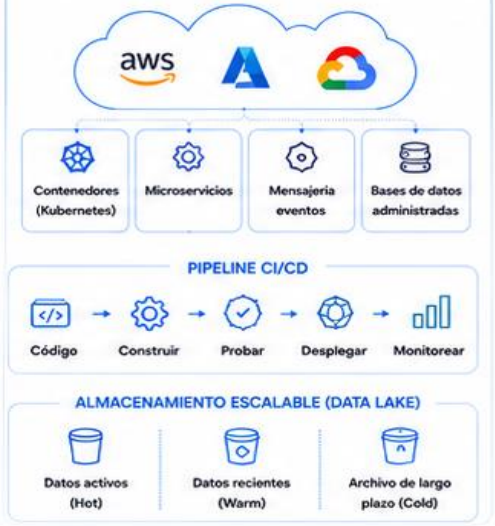
IMPACTO AL NEGOCIO

Mayor integración de sistemas, información en tiempo real entre áreas y decisiones más informadas.

3 ERA CLOUD Y DEVOPS CON CI/CD

La plataforma se moderniza en la nube. DevOps y CI/CD permiten entregas continuas y más rápidas.

ARQUITECTURA



EJEMPLO

Se procesan grandes volúmenes de información en la nube y se despliegan nuevas funciones sin interrupciones.

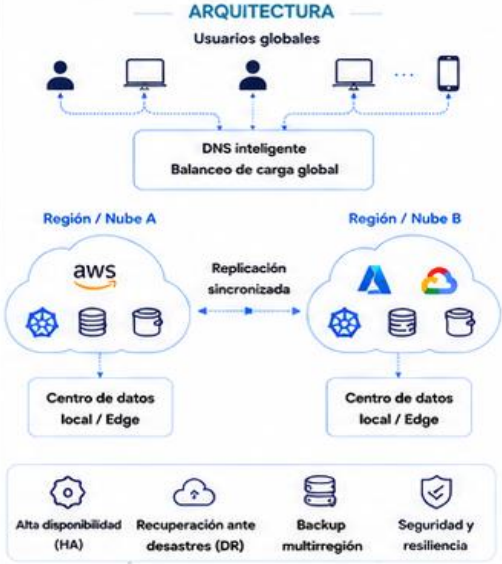
IMPACTO AL NEGOCIO

Más agilidad en el desarrollo, escalabilidad elástica y reducción de tiempos y costos de infraestructura.

4 ARQUITECTURA MULTICLOUD

La plataforma opera en múltiples nubes y regiones para asegurar disponibilidad, resiliencia y continuidad del negocio.

ARQUITECTURA



EJEMPLO:

Si una región falla, el servicio continúa disponible desde otra región sin afectar a los usuarios.

IMPACTO AL NEGOCIO

Servicio siempre disponible, recuperación rápida ante desastres y operación continua global.

5 APPLICATION AI-DRIVEN

La IA y los agentes inteligentes analizan datos del subsuelo y convierten la información en recomendaciones y mejores decisiones.

ARQUITECTURA

EJEMPLO

La IA ayuda a identificar zonas con mayor potencial, comparar escenarios y recomendar las mejores opciones para avanzar en un proyecto.

IMPACTO AL NEGOCIO

Decisiones más rápidas y precisas, mayor aprovechamiento de oportunidades y mejores resultados.

EVOLUCIÓN DE APPLICATIÓN SECURITY

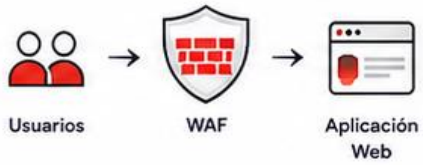
De la protección de aplicaciones web tradicionales a la seguridad de interacciones inteligentes y APIs

1 SEGURIDAD WAF

2000s – 2010s

Protección de aplicaciones web tradicionales

- SQL Injection
- XSS
- CSRF
- File Inclusion
- OWASP Top 10



ENFOQUE:
Proteger la capa web contra ataques a aplicaciones tradicionales.

2 SEGURIDAD DE API

2010s – 2016

Protección de APIs y servicios (exposición y abuso)

- API Discovery
- Shadow APIs
- API Abuse / BOLA
- Rate Limiting
- AuthN / AuthZ
- OWASP API Top 10

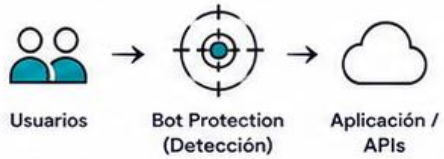
ENFOQUE:
Descubrir, proteger y controlar APIs en todo su ciclo de vida.

3 PROTECCIÓN DE BOTS Y PREVENCIÓN DE ABUSO

2016 – 2020

Protección contra automatización maliciosa y ataques a cuentas

- Bots Maliciosos
- Credential Stuffing
- Account Takeover
- Scraping
- Fraude Digital
- Behavioral Analytics



ENFOQUE:
Distinguir humanos de bots y proteger cuentas, sesiones y transacciones.

4 DISPONIBILIDAD Y RESILIENCIA

2016 – 2020+

Asegurar la disponibilidad, rendimiento y experiencia del usuario

- DDoS Protection
- GSLB / Load Balancing
- Health Monitoring
- Auto Scaling
- Fault Tolerance
- Global Availability

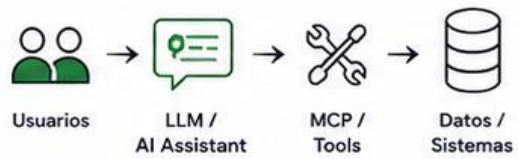
ENFOQUE:
Asegurar la disponibilidad continua de las aplicaciones en cualquier lugar y condición.

5 SEGURIDAD DE IA / MCP

2024+

Protección de interacciones con IA, LLMs y herramientas (MCP)

- MCP Security
- Prompt Injection
- Tool Abuse
- Data Leakage
- PII Protection
- AI Governance



ENFOQUE:
Proteger las interacciones con IA, modelos y herramientas que acceden a datos y sistemas.

¿POR QUÉ FORTIAPPSEC CONSIDERA CDN, GSLB Y DAST?

FortiAppSec va más allá del WAF. Integra capacidades clave para proteger, validar y asegurar que tu aplicación esté disponible, rápida y confiable para todos los usuarios.

1 PROTEGER
Durante el uso

FORTIAPPSEC
WAF & API PROTECTION

Protege la aplicación mientras está en uso

- Bloquea ataques a vulnerabilidades como SQLi, XSS, RCE y más
- Protege APIs y datos sensibles de accesos no autorizados
- Detecta y detiene bots maliciosos y automatización abusiva
- Mitiga ataques DDoS y picos de tráfico

Resultado:
Menos incidentes, menos fraude y datos protegidos.

2 VALIDAR
Antes y durante el ciclo de vida

FORTIDAST
DAST (PRUEBAS AUTOMÁTICAS) DE SEGURIDAD

Encuentra vulnerabilidades antes de que lo haga un atacante

- Pruebas dinámicas en la aplicación en ejecución (caja negra)
- Detecta vulnerabilidades de lógica de negocio y configuración
- Se integra al CI/CD para encontrar problemas antes de producción

TU APLICACIÓN
WEB / MÓVIL / APIS

3 ENTREGAR Y MANTENER DISPONIBLE
Siempre y para todos los usuarios

CDN
(RED DE ENTREGA DE CONTENIDO)

Acelera la entrega de contenido, reduce la latencia y absorbe grandes volúmenes de tráfico.

- Contenido más rápido para todos los usuarios
- Menor carga sobre los servidores de origen
- Mayor protección frente a picos de tráfico

GSLB
(BALANCEO GLOBAL INTELIGENTE)

Dirige a los usuarios al mejor sitio o región según disponibilidad, salud y ubicación.

- Alta disponibilidad y tolerancia a fallas
- Enrutamiento inteligente basado en salud y cercanía
- Continuidad del negocio sin interrupciones

Resultado:
Aplicación siempre disponible, rápida y resiliente a fallas.

USUARIOS
Empleados, clientes, partners y aplicaciones

→ Mejor experiencia y rendimiento → Datos y transacciones protegidos → Aplicación siempre disponible → Confianza y continuidad del negocio

FORTIAPPSEC integra estas capacidades para ofrecer PROTECCIÓN COMPLETA a tus aplicaciones.

FORTIAPPSEC: PROTEGE, VALIDA Y ASEGURA LA ENTREGA DE TUS APLICACIONES EN TODO SU CICLO DE VIDA.

WAF a WAAP: La superficie de ataque de la aplicación sigue creciendo

Se espera que las soluciones de aplicaciones web y protección de API gestionen hoy el tráfico de bots, aseguren APIs y mitiguen ataques DDoS

El 48% de las organizaciones tienen 100 o más aplicaciones únicas en su entorno

En promedio las empresas publican 25 actualizaciones de software en producción mensualmente

Más del 85% del tráfico web es tráfico de API

Casi la mitad del tráfico de internet es generado por bots

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Conceptos Clave

Casos de uso claves de seguridad y entrega de aplicaciones

Seguridad

- Protección de aplicaciones, API y MCP
- Exploits de Zero-day de GenAI
- Mitigación de bots y DDoS
- Cobertura global

Entrega

- Garantizar la disponibilidad y la resiliencia de las aplicaciones
- Entrega de aplicaciones a nivel global y en múltiples nubes

Optimización

- Análisis de amenazas para una clasificación y mitigación rápidas
- Operaciones asistidas por IA para identificar amenazas
- Automatización y personalizaciones de texto a script

EL HILO CONDUCTOR

Un modelo de madurez en cuatro niveles

Ubica al cliente en su nivel actual y muéstrale qué hace falta para subir al siguiente.

01

FUNDAMENTAL

Disponibilidad + WAF base

La app publicada, resiliente y con protección esencial L7.

02

ADVANCED

Zero-day, APIs y bots

Protección adaptativa con ML para amenazas que las firmas no ven.

03

PROFESSIONAL

Cumplimiento + multi-DC

PCI DSS 4.0, bots avanzados y continuidad entre data centers.

04

MASTER

Plataforma unificada + IA

Operación consolidada, IA asistida e integración Security Fabric.

ARQUITECTURA DE REFERENCIA

Dónde encajan FortiADC y FortiWeb / FortiAppSec

APLICACIONES MODERNAS

Web · Móvil · APIs · Microservicios · LLM / Agentes

FUNDAMENTAL

FortiADC

LB · SSL · DDoS L3/4

FortiWeb

WAF on-prem · K8s

FortiAppSec

WAAP edge · CDN

ADVANCED

ML / Zero-Day

Anomalía · sandbox

API Security

Discovery · GraphQL

Bot ML + ATO

Credential stuffing

PROFESSIONAL

ABP + PCI 4.0

Client-side · SOCaaS

GSLB multi-DC

Continuidad · DR

DAST

Vuln scan

MASTER

FortiAI Assist

Triage · explica

FortiCNAPP

Horizonte cross-sell

FortiCASB

Horizonte cross-sell

VISIBILIDAD · CORRELACIÓN · RESPUESTA FortiAnalyzer · FortiAI Assist · FortiGuard Labs · integración Security Fabric

ARQUITECTURA DE REFERENCIA

Dónde encajan FortiADC y FortiWeb / FortiAppSec

APLICACIONES MODERNAS

Web · Móvil · APIs · Microservicios · LLM / Agentes

FUNDAMENTAL

FortiADC

LB · SSL · DDoS L3/4

FortiWeb

WAF on-prem · K8s

FortiAppSec

WAAP edge · CDN

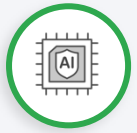
ADVANCED

ML / Zero-Day

Anomalía · sandbox

API Security

Discovery · GraphQL



Bot ML + ATO

Credential stuffing

PROFESSIONAL

ABP + PCI 4.0

Client-side · SOCaaS

GSLB multi-DC

Continuidad · DR

DAST

Vuln scan

MASTER

FortiAI Assist

Triage · explica

FortiCNAPP

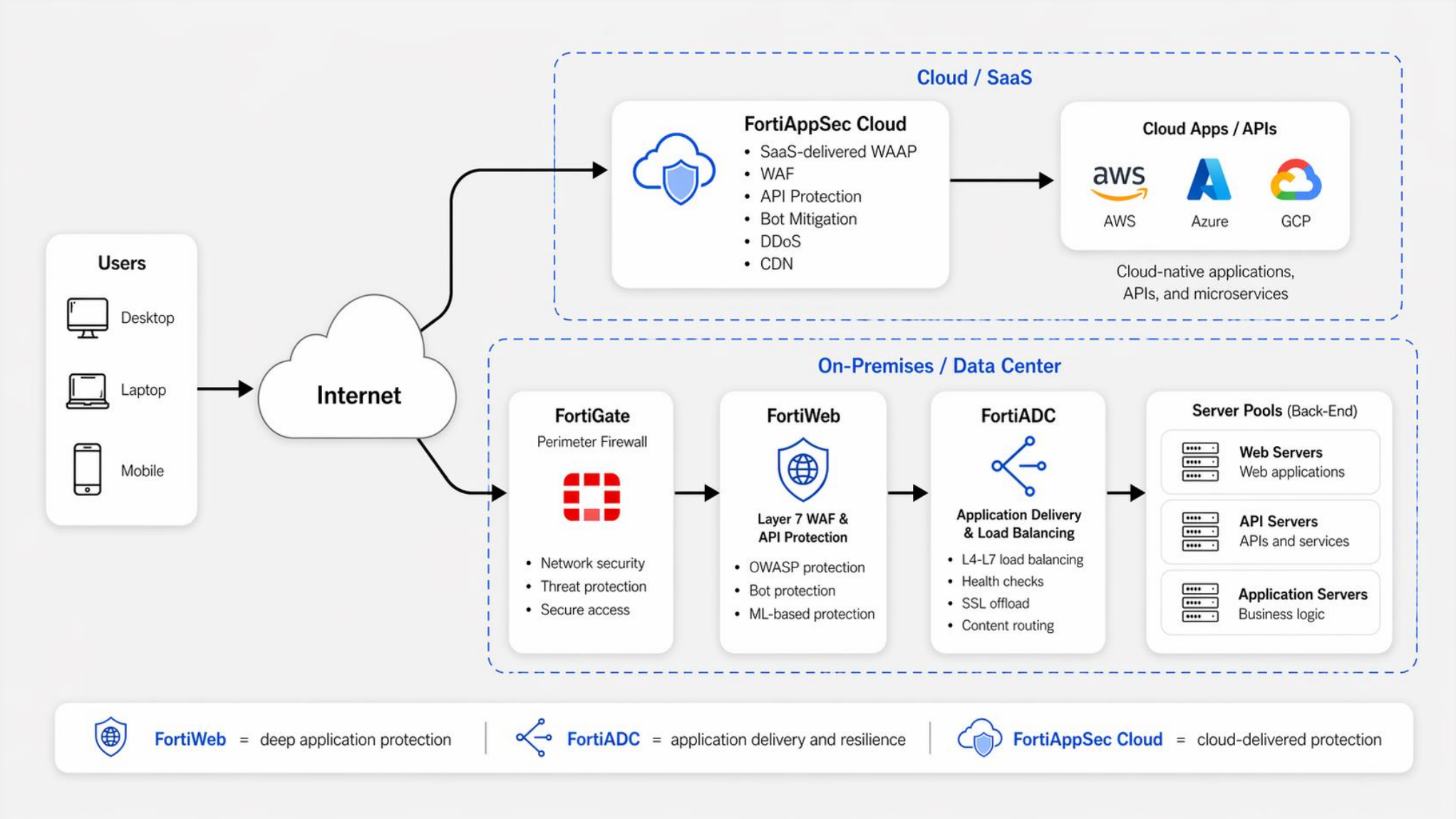
Horizonte cross-sell

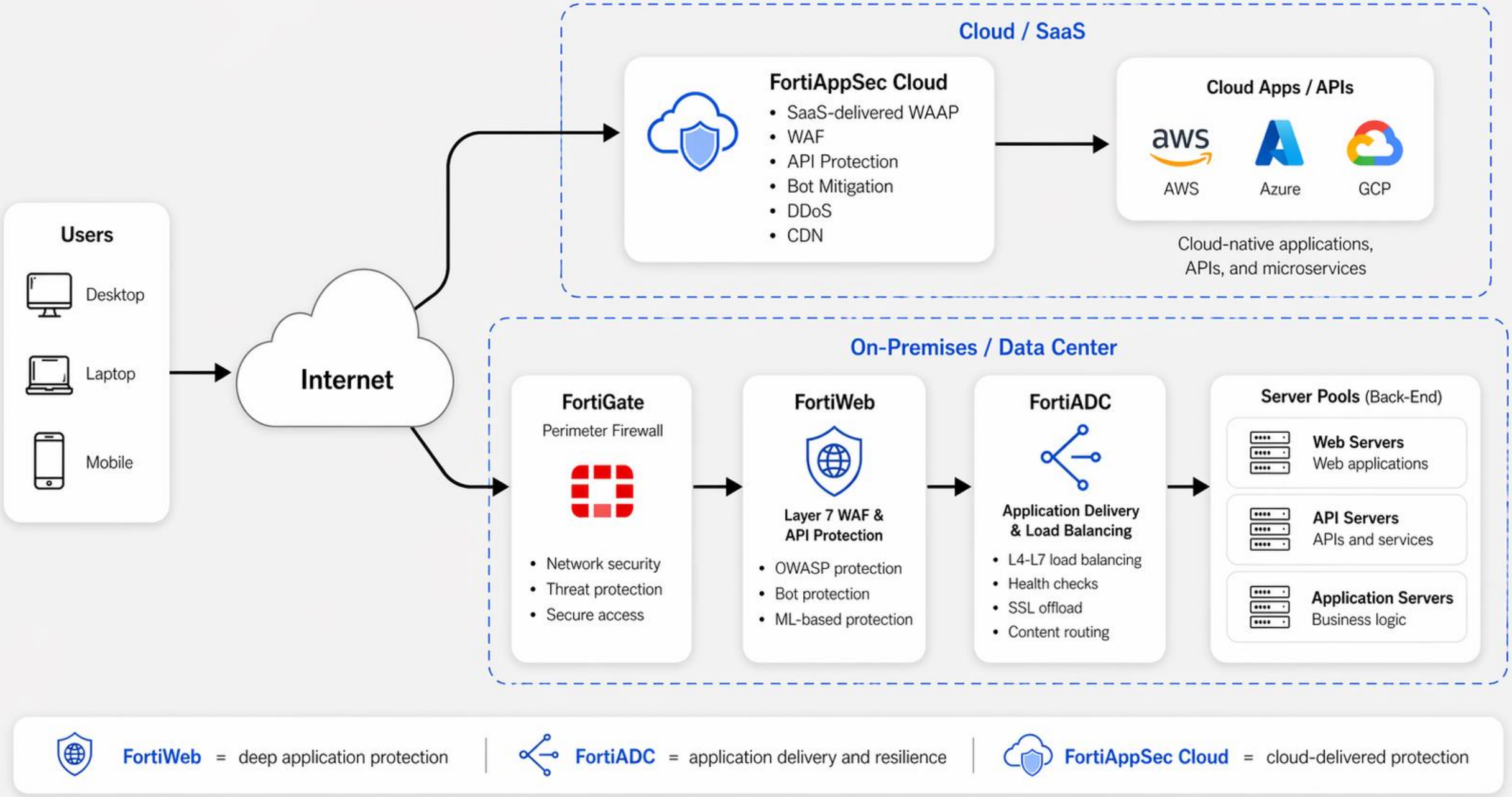
FortiCASB

Horizonte cross-sell

VISIBILIDAD · CORRELACIÓN · RESPUESTA FortiAnalyzer · FortiAI Assist · FortiGuard Labs · integración Security Fabric

Arquitectura de seguridad y entrega de aplicaciones de Fortinet




Cloud / SaaS
FortiAppSec Cloud
SaaS-delivered WAAP
WAF
API Protection
Bot Mitigation
DDoS
CDN
Cloud Apps / APIs
aws
AWS
Azure
GCP
Cloud-native applications, APIs, and microservices
Users
Desktop
Laptop
Mobile
Internet
On-Premises / Data Center
FortiGate
Perimeter Firewall
Network security
Threat protection
Secure access
FortiWeb
Layer 7 WAF & API Protection
OWASP protection
Bot protection
ML-based protection
FortiADC
Application Delivery & Load Balancing
L4-L7 load balancing
Health checks
SSL offload
Content routing
Server Pools (Back-End)
Web Servers
Web applications
API Servers
APIs and services
Application Servers
Business logic
FortiWeb = deep application protection
FortiADC = application delivery and resilience
FortiAppSec Cloud = cloud-delivered protection

01

MODELO DE MADUREZ · NIVEL 01

Fundamental · Disponibilidad + WAF base

ESCENARIO DEL CLIENTE

Qué está pasando

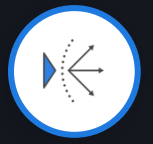
- Apps publicadas con balanceadores legados y costosos
- WAF básico o inexistente frente a las apps
- Exposición a OWASP Top 10 y caídas por picos de tráfico

CONTROL QUE HACE FALTA

Qué se necesita

- Entrega resiliente: LB L4/L7, SSL offload, health checks
- WAF por firmas, reputación IP/Geo, cumplimiento HTTP
- DDoS y validación de esquema básico de APIs

CÓMO LO RESOLVEMOS



FortiADC

LB L4/L7 · SSL offload · DDoS L3/L4 · health checks

FortiWeb

WAF on-prem / VM / K8s · inspección inline

FortiAppSec Standard

WAAP SaaS · OWASP · API schema · CDN · DDoS L7

PREGUNTA DE DISCOVERY: ¿Cómo publican y balancean sus apps hoy? ¿Tienen un WAF frente a ellas o confían solo en el firewall de red?

02

MODELO DE MADUREZ · NIVEL 02

Advanced · Zero-day, APIs y bots

ESCENARIO DEL CLIENTE

Qué está pasando

- APIs creciendo sin inventario ni control (shadow APIs)
- Bots, scraping y credential stuffing en aumento
- Ataques zero-day que las firmas no detectan

CONTROL QUE HACE FALTA

Qué se necesita

- ML / anomalía para zero-day
- Descubrimiento y protección de APIs (REST/GraphQL)
- Defensa de bots con ML, account takeover y DAST

CÓMO LO RESOLVEMOS

FortiAppSec Advanced

ML WAF zero-day · Threat Analytics AI · sandbox

API + Bot ML

API discovery · Gateway · GraphQL · ML Bot · ATO

DAST

Vulnerability & API scanning integrado

PREGUNTA DE DISCOVERY: ¿Protegen sus APIs además de la web? ¿Han visto bots, fraude o scraping en los logs de su WAF actual?

03

MODELO DE MADUREZ · NIVEL 03

Professional · Cumplimiento + resiliencia multi-DC

ESCENARIO DEL CLIENTE

Qué está pasando

- Manejan pagos y requieren PCI DSS 4.0
- Bots sofisticados de grado scrubbing-center
- Necesitan continuidad entre data centers / nubes

CONTROL QUE HACE FALTA

Qué se necesita

- Seguridad client-side automatizada (PCI 4.0)
- Advanced Bot Protection (ABP)
- GSLB multi-DC/multi-cloud y SOC gestionado

CÓMO LO RESOLVEMOS

FortiAppSec Enterprise

ABP · Client-Side PCI 4.0 · Waiting Room · SOCaaS

GSLB incluido

DNS LB · DNSSEC · health synthetic · failover

FortiADC GSLB

Continuidad activo-activo · link load balancing

PREGUNTA DE DISCOVERY: ¿Requieren cumplir PCI DSS 4.0? ¿Operan en varios DC o nubes? ¿Tienen SOC propio o lo necesitan como servicio?

04

MODELO DE MADUREZ · NIVEL 04

Master · Plataforma unificada + IA

ESCENARIO DEL CLIENTE

Qué está pasando

- Múltiples consolas y operación manual
- Sin correlación entre entrega, WAF y resto de seguridad
- Falta de visibilidad transversal del ciclo de la app

CONTROL QUE HACE FALTA

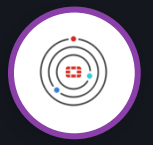
Qué se necesita

- Operación consolidada en una sola consola WAAP
- IA asistida: triage, explicación y remediación
- Integración Security Fabric y analítica de amenazas

CÓMO LO RESOLVEMOS

FortiAI Assist

Triage automatizado · explica alertas · sugiere fix



Security Fabric

FortiGate · FortiAnalyzer · FortiSandbox · FortiGuard

Horizonte AppSec

Cross-sell: FortiCNAPP · FortiCASB · cobertura total

PREGUNTA DE DISCOVERY: ¿Cuántas consolas operan hoy? ¿Pueden correlacionar un ataque a la app con el resto de su postura de seguridad?

AI-Powered

WEB APPLICATION AND API PROTECTION

API Discovery and Protection

API Discovery using URL clustering with schema awareness, automatic schema generation, Anomaly Detection (HMM+SVM)

Threat Analytics

Analyze million of events using ML to identify common characteristics and patterns and group them into meaningful security incidents

Web Protection

Zero day attack protection using two layer solution (HMM and SVM), Anomaly verification, continuous learning

FortiAI-Assist

An AI SOC agent that accelerate threat detection, analysis, and response by providing business context and recommendations

Bot Mitigation

Behavioral learning using ML SVM based on 13 different traffic dimensions, automated verification using training samples

Protección de Aplicaciones y API Impulsadas por IA

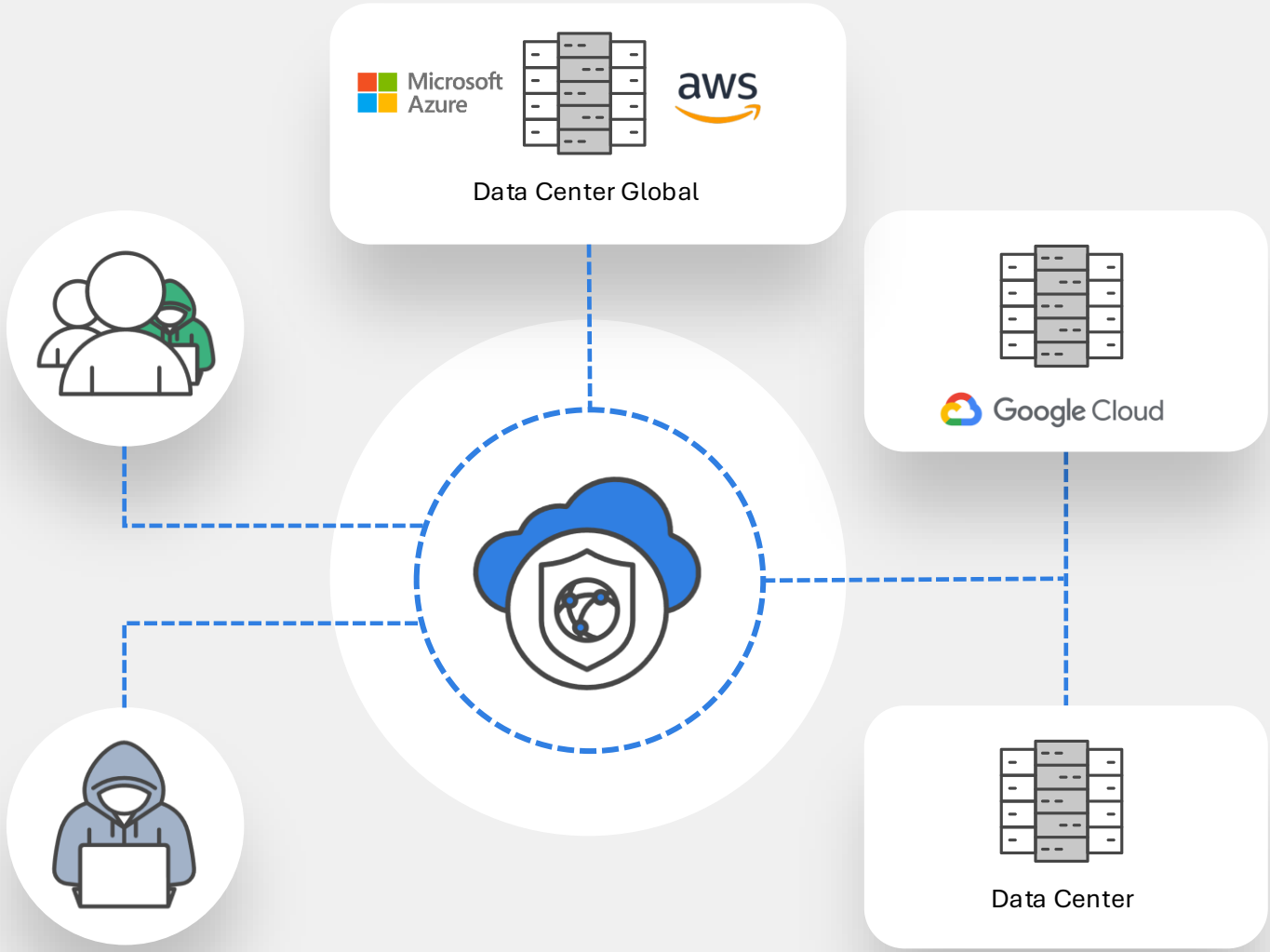
Application Protection

Protección de aplicaciones web

- Cobertura Top 10 de OWASP
- Protección de día cero
- Inteligencia de amenazas de FortiGuard

Descubrimiento y Protección de APIs

- Descubrimiento y catálogo
- Protección de API (XML/JSON):
- Acceso seguro y tokens
- Aplicación de esquemas y protocolos
- Detección de anomalías
- Protección contra amenazas



AI-Powered Bot Mitigation

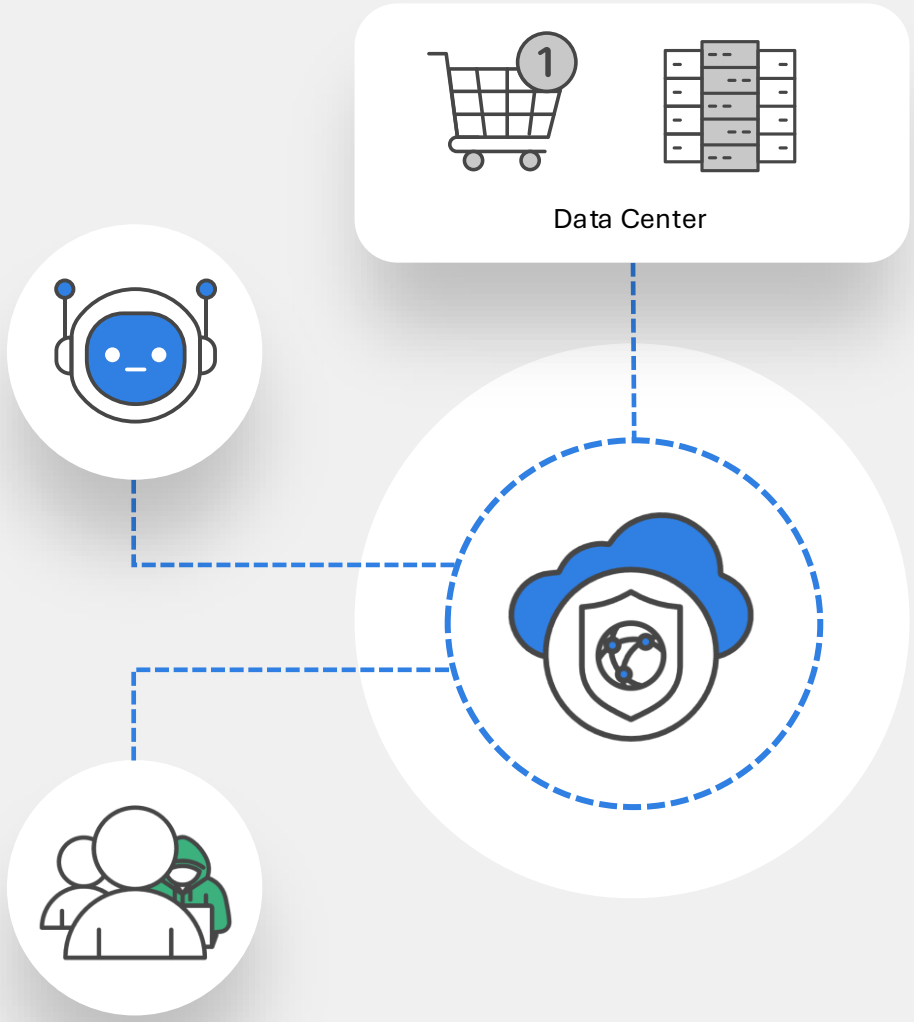
Bot Defense

Known Bots/ Signatures
- Crawler Detection/Limit

Browser Fingerprinting Detection
- Detecting Crawler-Specific Attributes
- Checking Browse/OS Inconsistencies

Biometric-based Detection
- Monitor client events

AI-Driven Behavioral Analysis
- Deep Learning & Data Correlation
- Multiple Dimensions Comparing

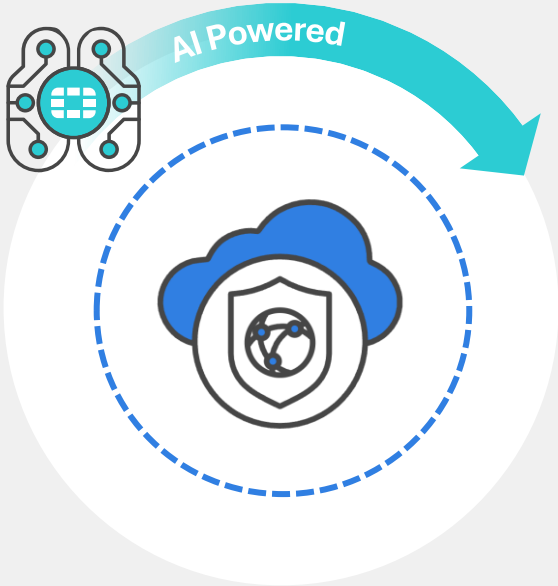


AI-Powered Threat Analytics

Threat Analytics

- **AI-based Threat Analytics**
  - Simplifies threat detection and response
  - Speeds up security alerts investigation
  - Focus on the most important threats
  - Insights provide suggestions to harden security based on findings
  - Ingests events from across your entire hybrid cloud environments
  - Alleviates alert fatigue

Speeds up Security alerts and investigation



Insights provide suggestions to harden security based on findings

Helps analysts **focus** on the most important threats - alleviates alert fatigue

Ingests events from across your entire hybrid cloud environments

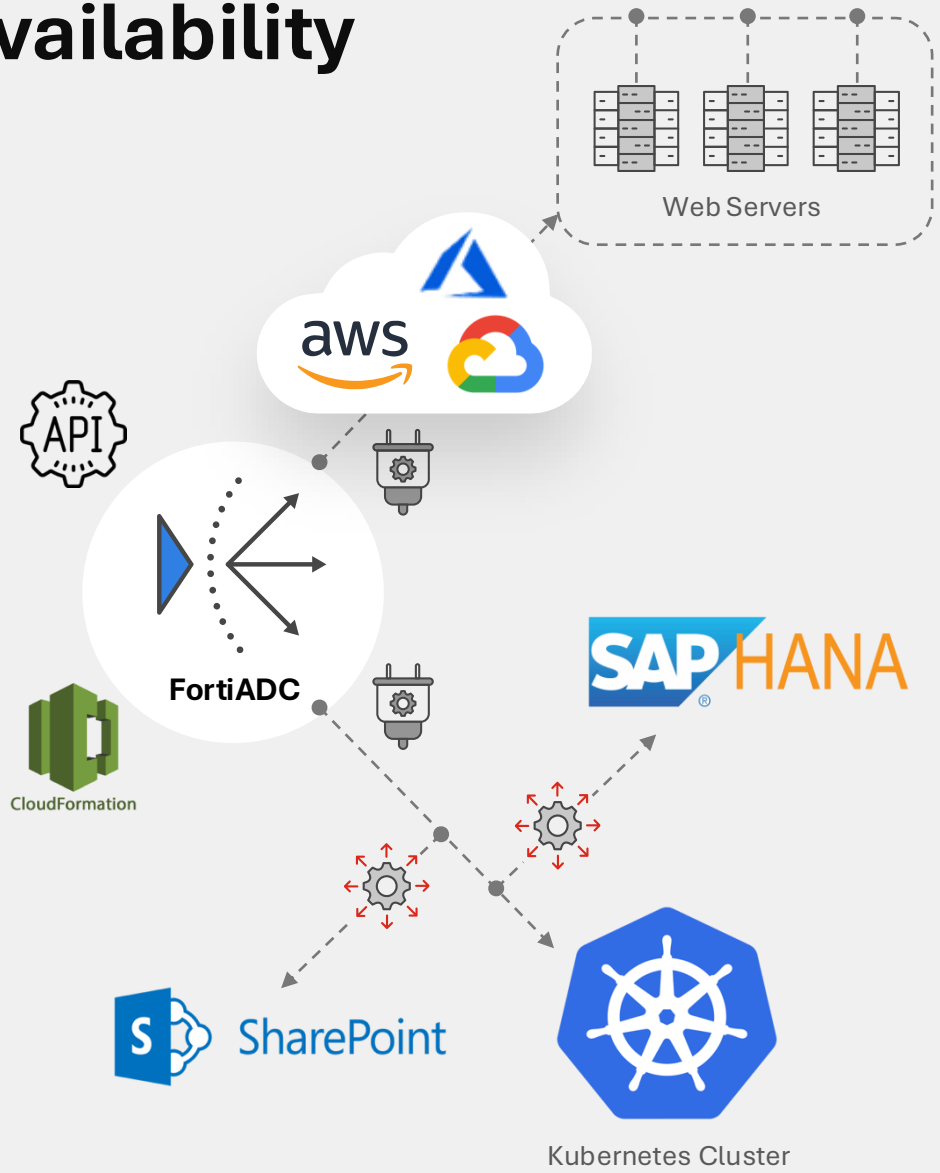
Application Delivery and Availability

Application Load Balancing
- L7 HTTP & HTTPS LB
- Advanced Health Check
- SSL Offloading and Inspection

Scripting & Automation
- Support any customer requirements
- React to real-time events via Automation

Global LB
- Ensuring Business Continuity
- Support traffic rerouting based on health checks, Geolocation, and application RTT

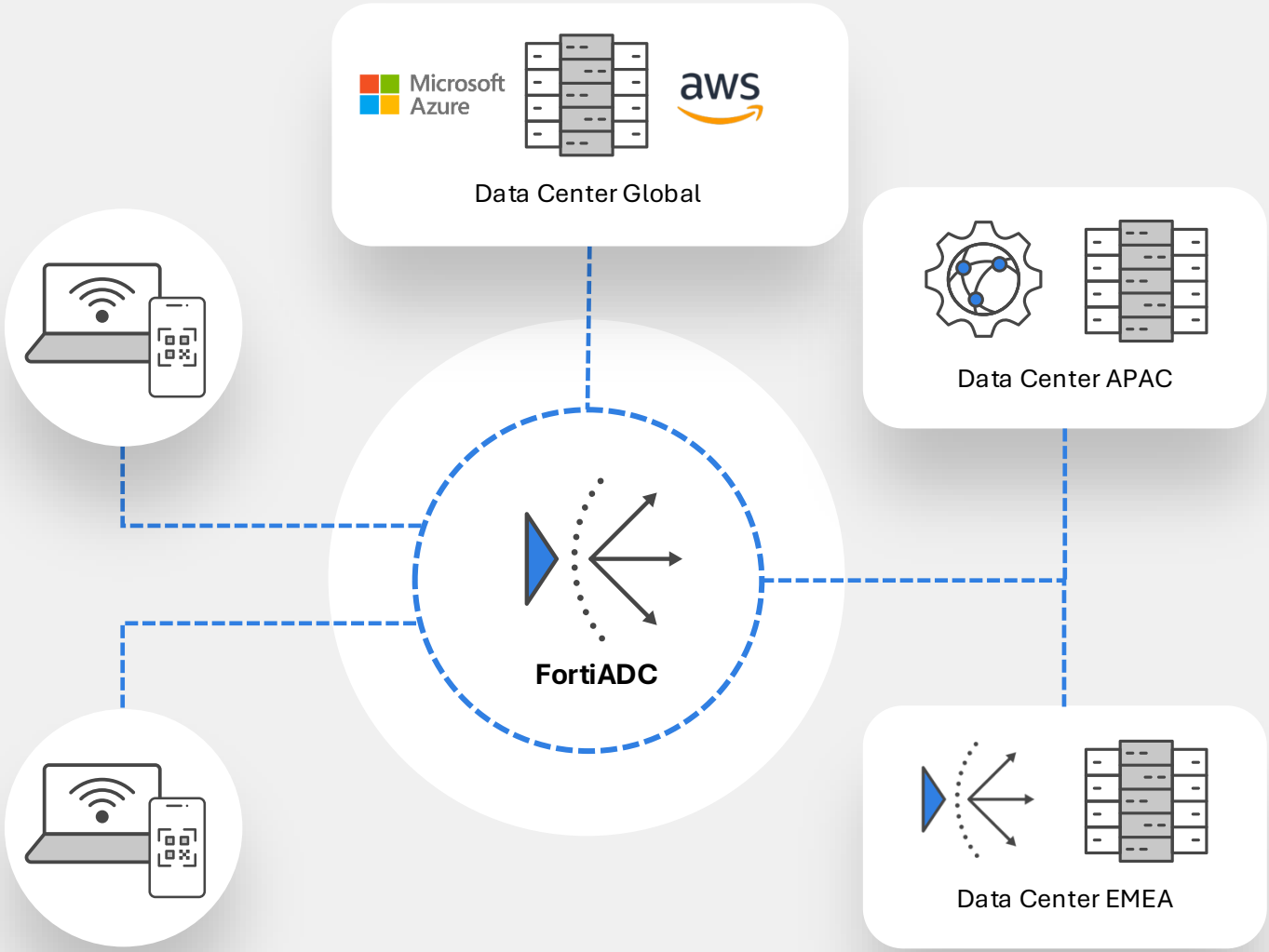
Optimization
- Improve User Quality of Experience
- Provide website performance enhancement tools



Global and Multi-Cloud Application Delivery

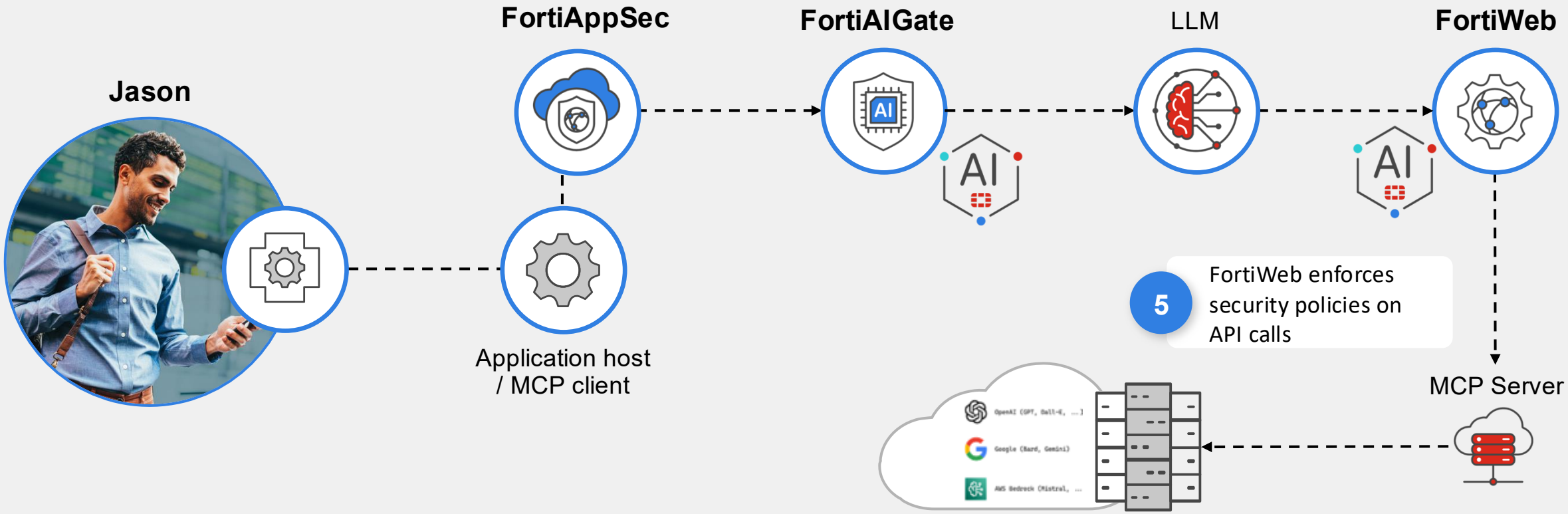
App Delivery

- **Global Load Balancing**
  - Application Availability and Visibility
  - Multi-Cloud Connect
  - Geo Location Awareness LB
  - Security Fabric Integration
  - Synthetic Testing
- **Content Delivery Networking**
  - Caching & Compression
  - Content-Based Location



Ampliación de la protección a las aplicaciones en la nube con inteligencia artificial.

1. User interacts with the app
2. App delivers user request to the training model
3. FortiAIGate sanitizes the input from malicious prompts
4. LLM gateway uses the MCP server to connect to external systems



FORTINET | COLOMBIA & ECUADOR

XPERTS26

Cuando la aplicación es la nueva frontera

Una sola Plataforma para proteger las aplicaciones