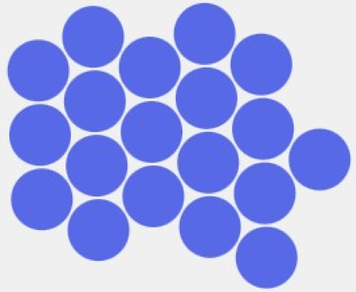
Mentimeter

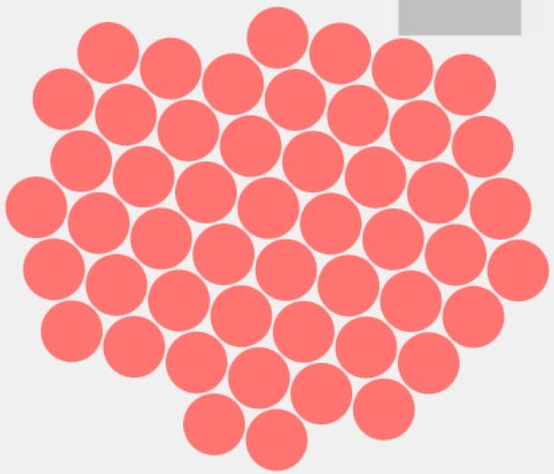
FORTINET

Mentimeter

¿Cuántos aquí ya están trabajando en nube pública hoy?



28% En-Premisa



72% Nube Pública

17

69 / 69

Mentimeter

FORTINET

Seguridad en la nube y entornos híbridos

André F. Moreno
Cloud Consulting System Engineer(CSE) LATAM

8

André F. Moreno

FORTINET®

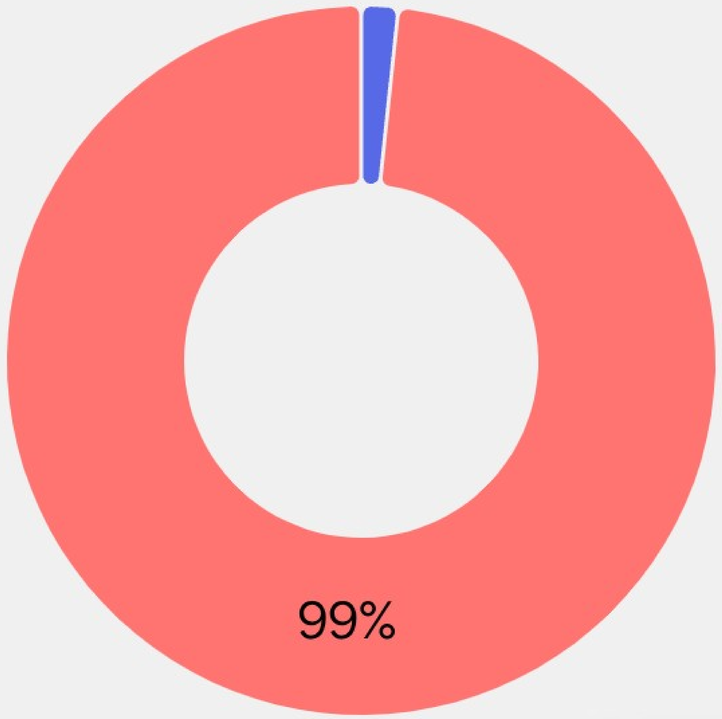
© Fortinet Inc. All R

Mentimeter

El desafío de
Asegurar La Nube

Mentimeter

¿Es lo mismo administrar infraestructura on-premises y en la nube pública?



1% SI

99% NO

3

70 / 70

En Premisas vs. Nube Publica

	En Premisas	Nube Publica
Perímetro	CLARO, DEFINIDO	INEXISTENTE
Cambio	LENTO ESTATICO	RAPIDO, DYNAMICO
Infraestructura	ENDPOINTS, SERVIDORES FISICOS	APIs, MICROSERVICIOS
Seguridad y Riesgo	RESPONSABILIDAD EXCLUSIVA DE SEGURIDAD	RESPONSABILIDAD COMPARTIDA, DEVSECOPS
Acceso	LIMITADO/CONFINADO A LA RED LOCAL	DESCENTRALIZADO DESDE CUALQUIER LUGAR

Mentimeter
27
2
© Fortinet Inc. All R

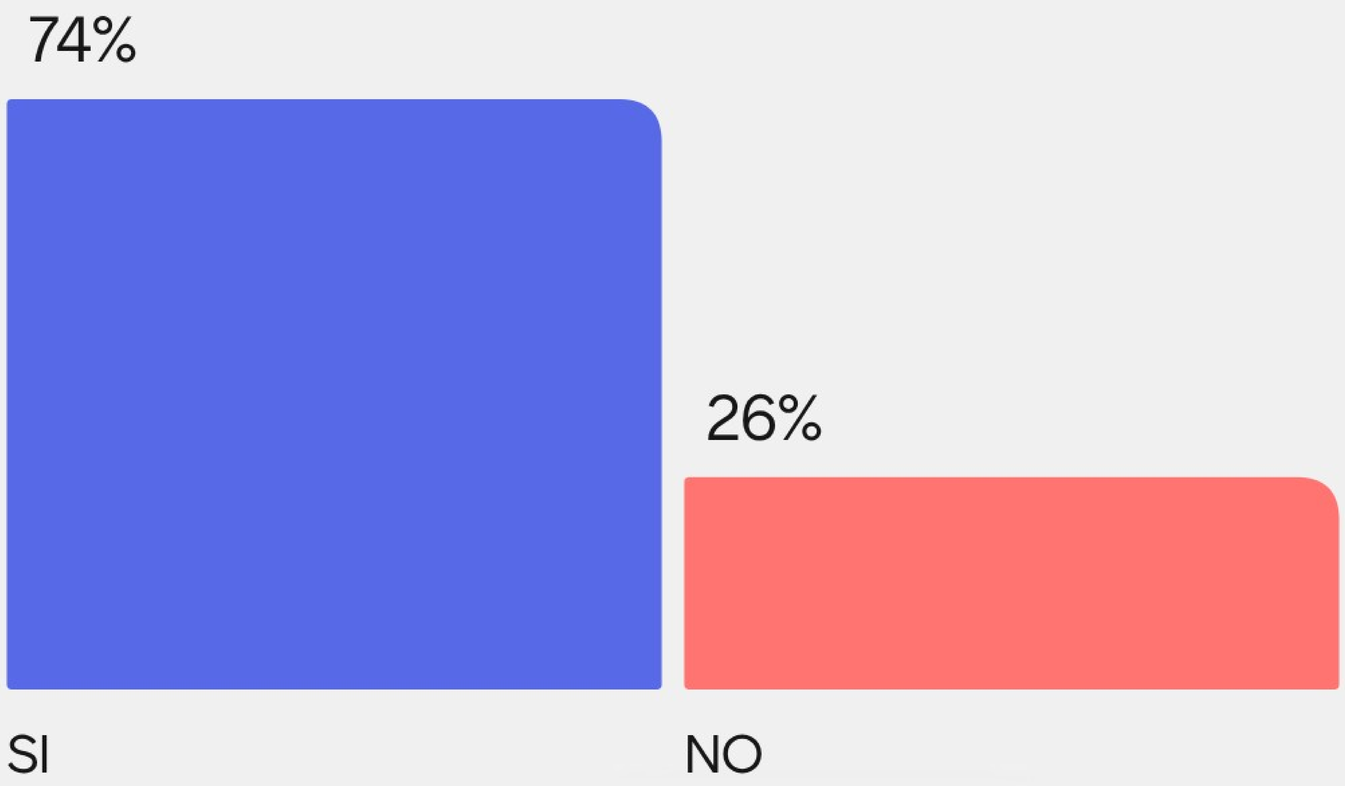
Evolución de la nube y los desafíos de seguridad

Complejidad de la nube	aplicaciones, nubes, instancias, permisos
Velocidad de desarrollo	código, commits, infraestructura, redes
Composición de aplicaciones	código abierto, dependencias complejas
Responsabilidad del código	desarrolladores definen contenedore, workloads y redes

© Fortinet Inc. All R

Mentimeter

¿Los Negocios son responsables de asegurar lo que despliegan en la Nube Publica?



9

62 / 62

La entrega de seguridad en la Nube Publica requiere una colaboración estrecha

+

aws

DATA DEL CLIENTE		
PLATFORMA, APPLICACIONES, IDENTIDAD & GESTINON DE ACCESOSS		
SISTEMA OPERATIVO, REDES, FIREWAL CONFIGURACIONES		
CIFRADO DE LADO DEL CLIENTE (DATOS EN TRANSITO E INTEGRIDAD) AUTENTICACION	CIFRADO DE LADO DEL SERVIDOR (SISTEMAS OPERATIVOS, Y/O DATOS)	PROTECCION DEL TRAFICO DE RED (CIFRADO, INTEGRIDAD, IDENTIDAD)
SOFTWARE		
COMPUTO	STORAGE	DATABASE	REDES
HARDWARE/INFRASTRUCTURA GLOBAL DEL LA NUBE		
REGIONES	ZONAS DE DISPONIBILIDAD	PERIMETROS DE NUBE

Cliente es responsable de las configuraciones de seguridad integrales **DENTRO** de la nube

Proveedor de **Nube** es responsable de la seguridad **DE** la nube

© Fortinet Inc. All R

LA VERDAD INCÓMODA

La Nube ha **roto el status quo de la ciberseguridad**

Configuraciones erróneas en la nube

600+
svcs de AWS, Azure y GCP

~500
configs de AWS T20 por instancia

3rd
vector de ataque inicial más común

Vulnerabilidades de código

29,785
New CVEs added to NVD since Jan 1

30%
YoY

65 days
average MTTR for a critical vulnerability

Compromiso de identidad

#1
vector de ataque en brechas reportadas

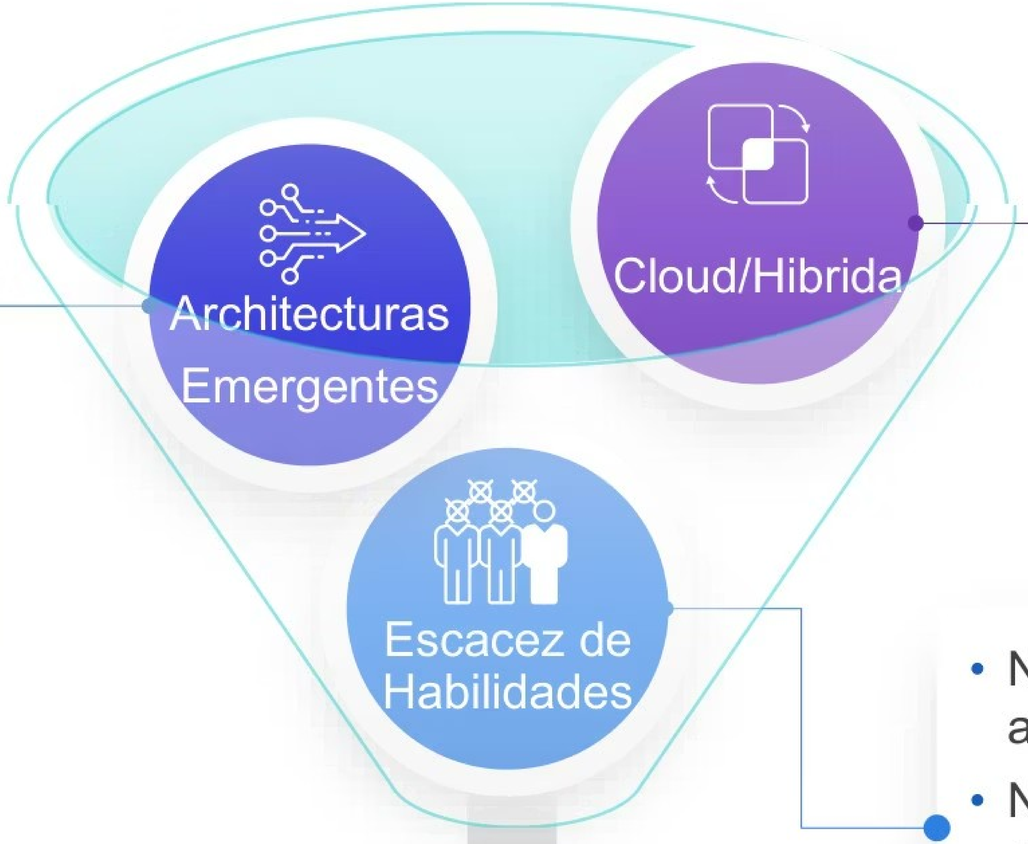
300%
credenciales robadas en intrusiones en la nube

68%
brechas involucran credenciales comprometidas

Mentimeter
11
© Fortinet Inc. All Rights Reserved.

Las arquitecturas de aplicaciones modernas crean puntos ciegos

Mentimeter



- Microservicisos
- Serverless
- Integraciónes
- LLMs

- Multiple entornos
- Gestion del Acceso
- SaaS

- Nuevas amenazas
- Nuevas solutiones
- Recursos limitados

Complexity

© Fortinet Inc. All R

Mentimeter

Los equipos de seguridad se están ahogando en el ruido y la complejidad de la nube

El cambio hacia la nube ha superado los enfoques tradicionales de seguridad.

Adopción rápida de la nube

Herramientas fragmentadas, alertas ruidosas y respuesta retrasada

La seguridad no puede seguir el ritmo de DevOps

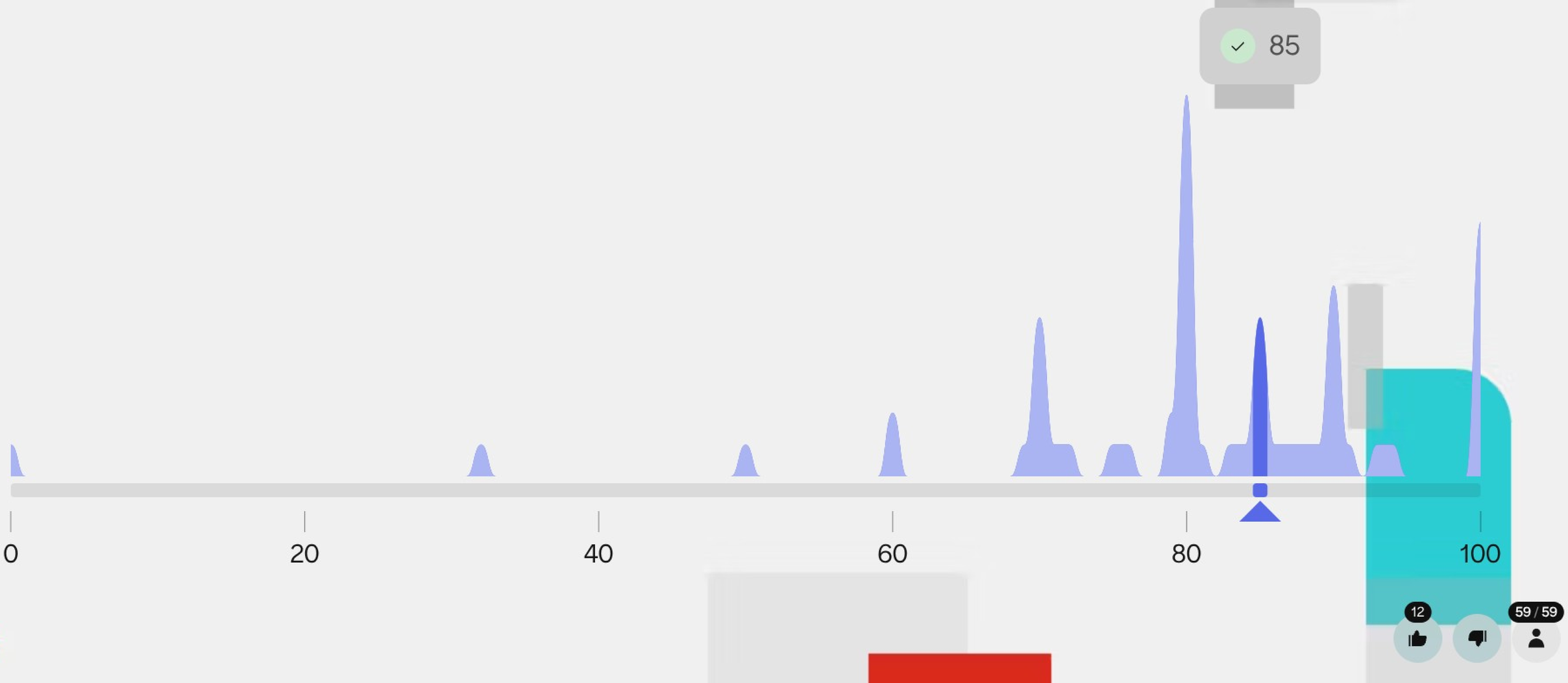
Visibilidad limitada, demasiadas herramientas desconectadas y una seguridad que no está alineada con el desarrollo.

4

© Fortinet Inc. All R

Mentimeter

¿Qué porcentaje del tráfico web creen que hoy corresponde a APIs entre sistemas?



La superficie de ataque de las aplicaciones sigue creciendo

Las soluciones de Protección de Aplicaciones Web y APIs hoy en día deben gestionar el tráfico de bots, asegurar APIs y mitigar ataques DDoS.

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

En promedio, las empresas publican **25 actualizaciones de software** en producción

Más del 85% del tráfico web es tráfico de APIs

Casi la mitad del tráfico de internet es generado por bots

© Fortinet Inc. All R

Fundamentos de la solución para casos de uso críticos

Seguridad de aplicaciones web consolidada

Bloquear amenazas conocidas y desconocidas de adversarios humanos, bots sofisticados y herramientas de IA generativa. Descubrir y proteger APIs.

Protección integral y precisa del Top 10 de OWASP

Aplicación de políticas agnóstica a la nube

Aplicación consistente en centros de datos, entornos híbridos y multicloud.

Gestión centralizada y unificada

Entrega segura de aplicaciones

Garantizar la disponibilidad de las aplicaciones, optimizar el rendimiento y acelerar la entrega de contenido.

CDN y protección contra DDoS

Operaciones simplificadas

Integrar, automatizar y analizar patrones sospechosos, obtiene visibilidad y prioriza mitigaciones.

Reduce la fatiga de alertas, mejora la productividad del SOC

Mentimeter
3
© Fortinet Inc. All R

Cómo abordar este desafío

Identificar, priorizar y resolver riesgos y amenazas en aplicaciones nativas de la nube

Minimizar la superficie de ataque

Obtener visibilidad integral y reducir de forma proactiva vulnerabilidades, configuraciones erróneas y privilegios excesivos sin ralentizar el desarrollo.

Monitorear riesgos continuamente

Evaluar continuamente máquinas virtuales, contenedores y cargas de trabajo de Kubernetes para identificar riesgos activos antes de que sean explotados.

Reducir el impacto de las amenazas

Detectar, investigar y responder rápidamente a comportamientos inusuales y amenazas activas, incluyendo el uso de credenciales comprometidas, ransomware en la nube y cryptomining.

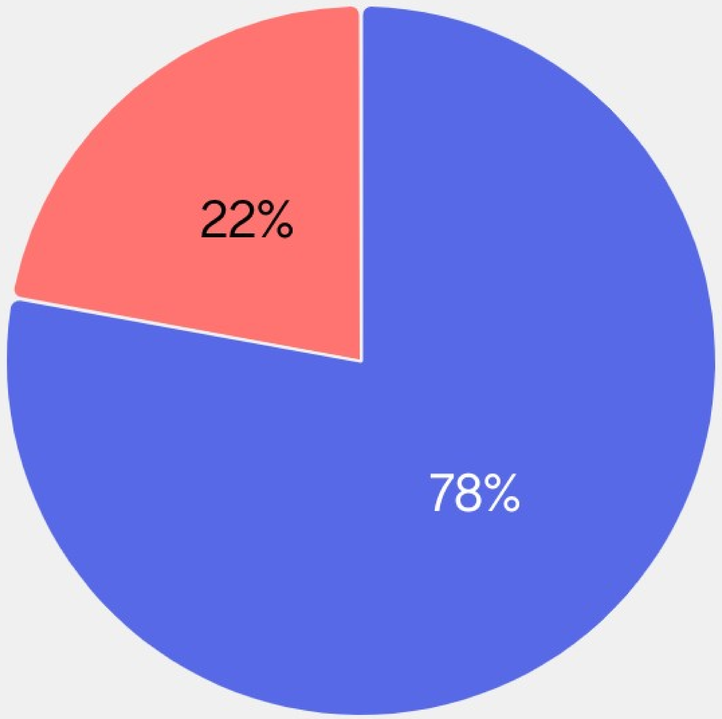
Mentimeter

5

© Fortinet Inc. All R

Mentimeter

¿Hoy tienen una plataforma integrada o múltiples herramientas separadas?



78% Herramientas Separada

22% Plataforma Integrada

7

50 / 50

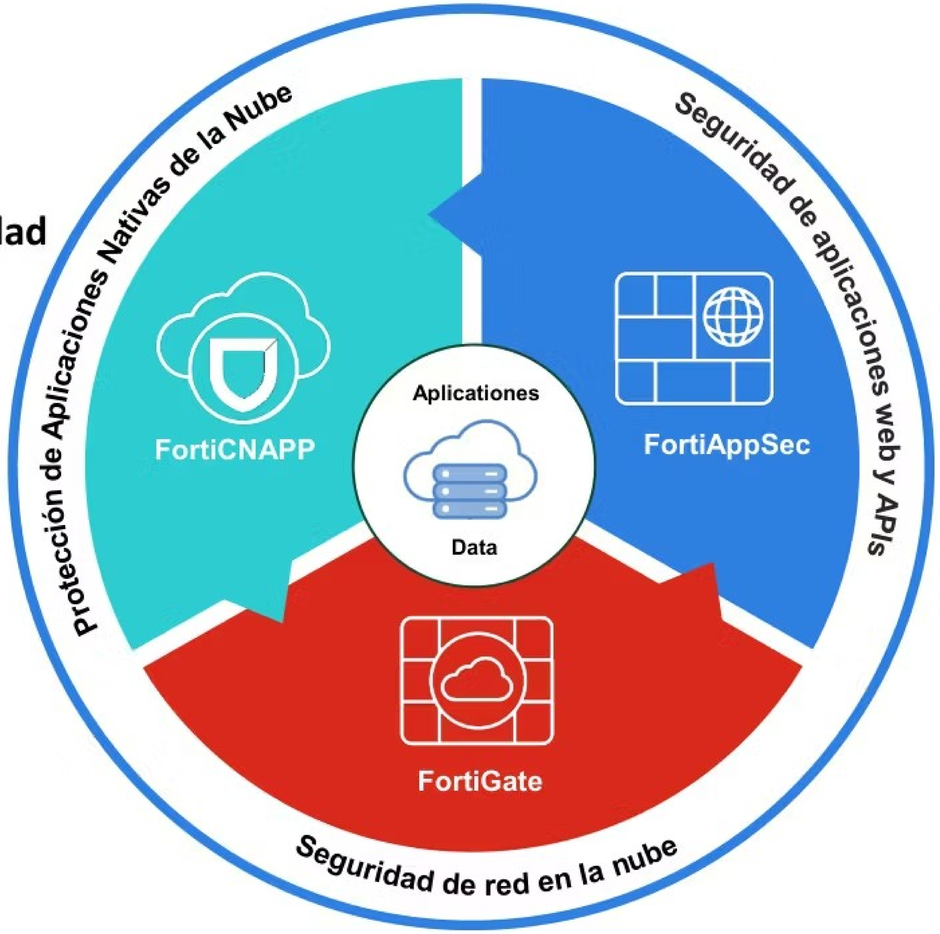
Mentimeter

Como
Asegurar La Nube

Seguridad integrada desde el código hasta la nube

Protección a profundidad de 360° en la nube contra todos los vectores de amenazas y riesgos

Asegurar todo, desde el código hasta la nube, más rápido, con **contexto y visibilidad incomparables en una única plataforma unificada.**



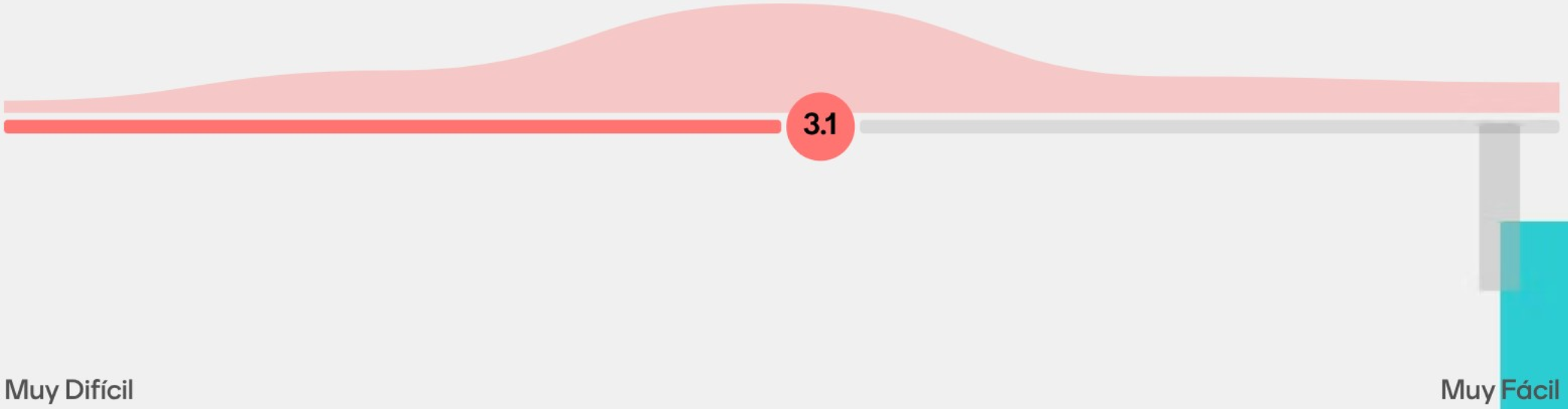
Plataforma integrada impulsada por IA/ML para proteger aplicaciones web y APIs críticas para el negocio frente a ataques que explotan vulnerabilidades conocidas y desconocidas.

Lograr visibilidad de red y la aplicación de **políticas de seguridad consistentes** en entornos de nube privada, pública y telco.

© Fortinet Inc. All R

Mentimeter

¿Qué tan difícil es correlacionar eventos entre sus soluciones actuales?



3

38 / 38

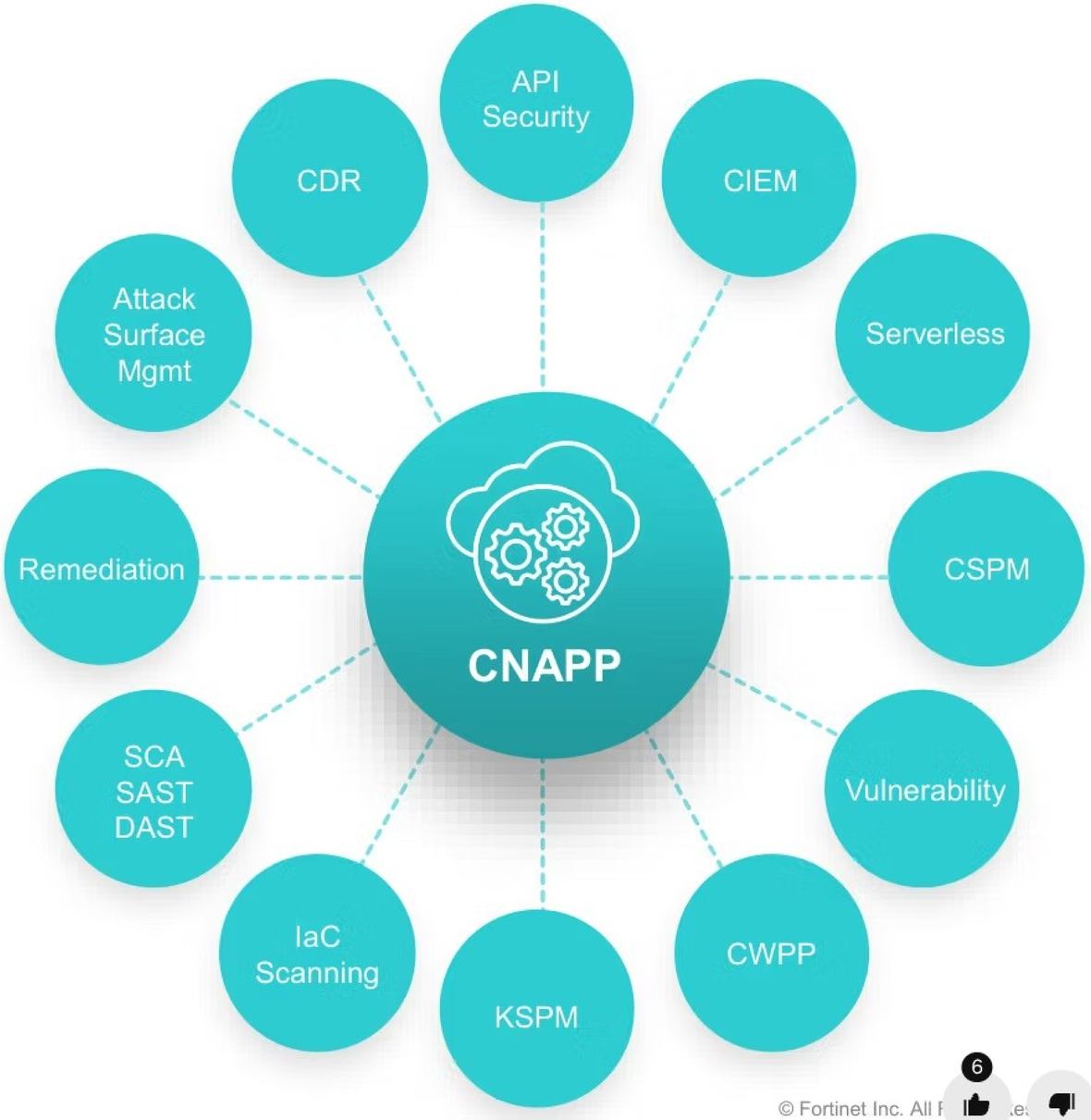
Cloud-Native Application Protection Platform (CNAPP)

Un término acuñado por Gartner

CNAPP:

"Cloud-native application protection platforms (CNAPPs) son un conjunto unificado y estrechamente integrado de capacidades de seguridad y cumplimiento diseñadas para asegurar y proteger aplicaciones nativas de la nube a lo largo del desarrollo y la producción.

Gartner



© Fortinet Inc. All R

Desde la primera línea de código hasta la nube: la seguridad nunca se detiene

El desarrollo asistido por IA acelera la entrega y el riesgo

Código → **Compilación (Build)** → **Despliegue** → **Ejecución (Run)** → **Monitor**

El código generado por IA puede introducir vulnerabilidades ocultas o filtrar datos sensibles.

Las canalizaciones automatizadas de IA pueden incorporar componentes no verificados o permisos excesivos.

Los despliegues impulsados por IA pueden omitir controles de seguridad y crear configuraciones erróneas.

Las cargas de trabajo de IA pueden exponer datos sensibles o ser manipuladas mediante inyección de prompts.

Las herramientas tradicionales no detectan riesgos específicos de IA y saturan a los equipos con ruido.

© Fortinet Inc. All R

Los nuevos puntos ciegos del desarrollo impulsado por IA

Dónde se encuentran las brechas actuales

© Fortinet Inc. All R

Capacidades clave de CNAPP

Una plataforma unificada para asegurar desde el código hasta la nube

Código

- Analizar código y APIs en desarrollo
- Identificar vulnerabilidades, malware y configuraciones erróneas
- Prevenir despliegues de aplicaciones fuera de cumplimiento

Despliegue

- Evaluar configuraciónes de la infraestructura en la nube
- Analizar identidades y sus permisos
- Priorizar riesgos mediante análisis de rutas de ataque

Ejecución (Run)

- Monitoreo continuo de exposiciones y data sensitiva
- Detectar comportamientos inusuales y amenazas activas
- Comprender procesos en ejecución y mapear conexiones de red

Mentimeter
6
© Fortinet Inc. All R

Capacidades clave de CNAPP

Una plataforma unificada para asegurar desde el código hasta la nube

Código

- Analizar código y APIs en desarrollo
- Identificar vulnerabilidades, malware y configuraciones erróneas
- Prevenir despliegues de aplicaciones fuera de cumplimiento

Seguridad del código

Análisis de composición de software (SCA)	Pruebas de seguridad de aplicaciones estáticas (SAST)	Seguridad de infraestructura como código (IaC)

Despliegue

- Evaluar configuraciónes de la infraestructura en la nube
- Analizar identidades y sus permisos
- Priorizar riesgos mediante análisis de rutas de ataque

Configuración de la nube

Evaluación de vulnerabilidades	Gestión de postura de seguridad (CSPM)	Gestión de entidades de infraestructura en la nube (CIEM)

Ejecución (Run)

- Monitoreo continuo de exposiciones y data sensitiva
- Detectar comportamientos inusuales y amenazas activas
- Comprender procesos en ejecución y mapear conexiones de red

Protección en tiempo de ejecución

Protección de Workload en la nube (CWP)	Detección y respuesta en la nube (CDR)

Mentimeter

5

© Fortinet Inc. All R

Mentimeter

¿Cuánto tiempo tardan hoy en detectar un incidente crítico?

5

31 / 31

El valor de la detección de amenazas en tiempo real

De horas a minutos

Mentimeter
AI-Driven Threat Detection

La alerta más rápida acelera la detección de anomalías y la respuesta a amenazas antes de que los atacantes puedan escalar sus acciones.

Detección más rápida = respuesta más rápida

Reducir la latencia de las alertas de horas a menos de 15 minutos permite al equipo de seguridad detener un ataque en curso antes de que cause pérdidas financieras o daños reputacionales.

Reducción del riesgo operativo

La visibilidad inmediata del comportamiento malicioso ayuda a proteger los sistemas en producción y los datos sensibles de los clientes.

Menores costos

Bloquea la activación no autorizada de recursos de cómputo, evitando potencialmente miles de dólares en cargos inesperados en la nube.

Postura de seguridad más sólida

Demuestra una defensa proactiva en tiempo real durante auditorías y fortalece la madurez general de la seguridad en la nube.

© Fortinet Inc. All R

Beneficios para el negocio

Mentimeter

Reducción de la complejidad

Simplifica la gestión de múltiples soluciones de seguridad en entornos híbridos y multicloud.

Preparado para ataques de GenIA

Protección adaptativa contra exploits de día cero en aumento y ataques sofisticados de bots dirigidos a aplicaciones web y APIs.

Disponibilidad Global

Garantiza una disponibilidad consistente de las aplicaciones en diversos entornos globales.

Cumplimiento

Proporciona visibilidad de 360° para la gestión del cumplimiento en todas las aplicaciones.

5

© Fortinet Inc. All R

Mentimeter

Si pudieran resolver SOLO un problema hoy, ¿cuál sería?

1

28 / 28

Mentimeter

“Las organizaciones que liderarán el futuro no serán las que adopten la nube más rápido, sino las que la aseguren mejor.”

Cloud CSE

5

Mentimeter

Si quieres profundizar en cómo proteger tu entorno cloud, te esperamos en el stand de

FORTINET®

smartbytes