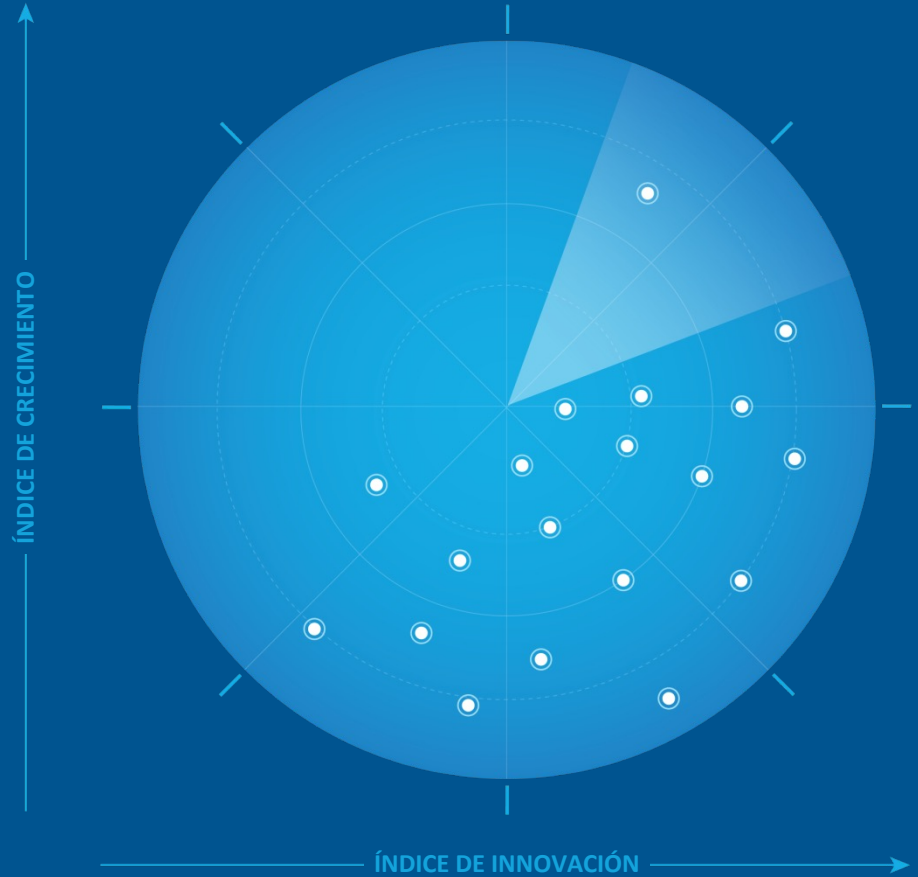


Frost Radar™: plataformas de protección de aplicaciones nativas en la nube, 2022

Un sistema de análisis comparativo para animar a las empresas a actuar: la innovación como motor de generación de oportunidades y de crecimiento



Autor: Anh Tien Vu
Responsable del sector, ciberseguridad internacional

PD8C-74
Noviembre de 2022

Imperativos estratégicos y entorno de crecimiento



Imperativos estratégicos

El uso de la computación en la nube, con una variedad de modelos y servicios disponibles, se está imponiendo en el entorno empresarial. La migración acelerada a la nube ha permitido a las empresas efectuar la transición al mundo digital y simplificar sus infraestructuras de TI y sus operaciones.

El uso de la computación en la nube está transformando el ciclo de vida de desarrollo de aplicaciones, las operaciones de seguridad y la forma en que las organizaciones crean, utilizan y gestionan la infraestructura back-end y las aplicaciones destinadas al cliente (front-end), con tecnologías nativas de la nube, como contenedores/Kubernetes, serverless, infraestructura como código (IaC) y otras plataformas de integración continua/entrega continua (CI/CD), para la administración, aplicación, desarrollo y despliegue en la nube.

Con el acento puesto en las tecnologías de desarrollo de aplicaciones nativas en la nube, las organizaciones están cambiando el modelo de desarrollo de aplicaciones monolítico tradicional por una arquitectura de microservicios y un enfoque con contenedores que emplea más bibliotecas y dependencias de código abierto.

Las tecnologías de contenedores/Kubernetes y la computación serverless están cambiando las estrategias de desarrollo de aplicaciones, ya que permiten a las organizaciones diseñar, desarrollar, probar y lanzar sus aplicaciones al mercado con flexibilidad, mejorando así la experiencia del cliente. [El informe anual de la Cloud Native Computing Foundation \(CNCF\) de 2021](#) mostró que el 96 % de las organizaciones están usando o evaluando Kubernetes y que el 93 % usan o prevén usar contenedores en sus procesos de producción. Sin embargo, el uso de software, bibliotecas/dependencias y registros de código abierto ha generado preocupación e introducido más amenazas para la seguridad, ya que estos artefactos de aplicaciones siguen expuestos a la vulnerabilidad de las imágenes de contenedores, los fallos de seguridad de hosts, la inyección de código (para aplicaciones serverless) y los problemas relacionados con el incumplimiento de normativas.

Imperativos estratégicos (continuación)

El aumento de complejidad del entorno híbrido y multinube, así como la expansión de la superficie de ataque y la multiplicación de los retos relacionados con las operaciones de seguridad exigen el uso de una plataforma integrada y nativa en la nube que pueda proporcionar a las empresas visibilidad, control y protección, y garantizar la seguridad de las arquitecturas de computación en la nube actuales (máquinas virtuales, contenedores, Kubernetes, entornos serverless), así como integrar la seguridad en el ciclo de vida de desarrollo de software y ayudar a las organizaciones a cumplir las normativas de manera satisfactoria. Por todo ello, el enfoque de la seguridad tradicional ya no funciona, ya que no está diseñado para admitir la microsegmentación ni es lo suficientemente robusto para adaptarse a los cambios en las aplicaciones, en particular en los entornos de contenedores y serverless.

Como resultado, el CNCF reclama un cambio de paradigma para adoptar un modelo de seguridad denominado "shift-left and shield-right" que permita proteger las aplicaciones nativas en la nube, acercando la seguridad a las cargas dinámicas identificadas en función de atributos y metadatos, como las etiquetas e identificadores. Este modelo exige que la seguridad se integre en las primeras etapas y a lo largo del ciclo de desarrollo de aplicaciones, en lugar de únicamente en las últimas fases, así como una administración de la seguridad para el entorno de nube en el que se despliegan y se ejecutan las aplicaciones, lo que acentúa la necesidad de una plataforma de protección de aplicaciones nativas en la nube, o CNAAP.

CNAPP ofrece a las organizaciones una plataforma de seguridad integrada para responder a estas amenazas de seguridad, en lugar de soluciones independientes, como las soluciones CSPM (gestión de la postura de seguridad de la nube), CWPP (plataforma de protección de cargas de trabajo en la nube) o de gestión de vulnerabilidades. Una plataforma CNAPP también facilita la colaboración entre los equipos de seguridad, TI/plataforma y desarrollo, con el fin de mejorar la productividad y gestionar de manera más eficiente los riesgos a los que se exponen sus entornos de nube.

Fuente: Frost & Sullivan

Entorno de crecimiento

En 2021 el mercado mundial de CNAPP registró una cifra de negocio de 1720,6 millones de dólares, lo que representa un crecimiento interanual del 48,8 %. Frost & Sullivan prevé que esta tendencia alcista continúe, con una tasa de crecimiento anual compuesto del 25,7 % desde 2021 hasta 2026, y que los ingresos alcancen los 5406,8 millones de dólares en 2026, debido al aumento de la demanda de una plataforma de seguridad de la nube unificada capaz de reforzar la protección de la infraestructura de la nube, así como las aplicaciones y los datos a lo largo de su ciclo de vida completo.

En general, las empresas llevan tiempo adoptando componentes de CNAPP individuales, principalmente soluciones CSPM para la visibilidad y el control de la seguridad en la nube, y CWPP para la protección en tiempo de ejecución y el cumplimiento de normativas. La inversión en seguridad de DevOps ha aumentado últimamente, debido a la necesidad de anticipar la seguridad (shift-left) para inyectar protección en las etapas iniciales del ciclo de vida de desarrollo de software. Del mismo modo, las soluciones de gestión de derechos sobre la infraestructura de nube (CIEM, Cloud Infrastructure Entitlement Management) y de seguridad de redes en la nube (CNWS, Cloud Networks Security) son muy utilizadas por empresas que han adoptado recientemente la nube y que antes usaban soluciones de sus proveedores de servicios de la nube.

Dicho esto, en todo el mundo las organizaciones han realizado inversiones importantes en distintas formas de CNAPP. La mayoría se destinan a productos individuales para casos de uso y problemas específicos. El concepto de CNAPP, que consiste en consolidar todas estas herramientas, sigue siendo nuevo, al igual que su acrónimo, lo que suscita confusión entre los usuarios potenciales y hace que la inversión se afronte con cautela. Sin embargo, la adopción acelerada de los servicios en la nube y las tecnologías de desarrollo de aplicaciones nativas en la nube, junto con el incremento de la superficie de ataque en el entorno de nube incentivarán el gasto en las tecnologías de seguridad de la nube, en general, y en las plataformas CNAPP, en particular.

Fuente: Frost & Sullivan

Entorno de crecimiento (continuación)

Numerosas organizaciones, en especial las más maduras, son conscientes de que el riesgo que presentan las aplicaciones aisladas y el uso de código abierto, así como la incapacidad de responder rápidamente a las amenazas contra infraestructuras y cargas de trabajo, pueden generar lagunas en la seguridad y aumentar la complejidad para sus equipos. La necesidad de identificar, priorizar y solucionar el riesgo de manera centralizada intensificará la demanda de soluciones CNAPP.

Para afrontar de manera conjunta los riesgos de seguridad y de incumplimiento de normativas, se necesita una sola plataforma que aúne una mejor protección, una visibilidad granular y una gestión de riesgos eficiente. Esto es consecuencia de la generalización de la estrategia multinube, la necesidad continua de proteger las cargas de trabajo frente a ataques y la presión para centralizar la implementación coherente de directivas entre los distintos entornos: infraestructura en la nube, los contenedores/Kubernetes, IaC o las canalizaciones CI/CD.

Cada vez es más acuciante la necesidad de mejorar la integración de las soluciones CNAPP con el ciclo de desarrollo de software de DevOps y con las plataformas de canalizaciones CI/CD, con el fin de aplicar el enfoque de seguridad desde el diseño (shift-left) y en cada fase de la creación del software (desarrollo, testing y lanzamiento). La integración de CNAPP con DevOps pretende abordar las preocupaciones por el análisis de artefactos de aplicaciones (testing de seguridad de aplicaciones estáticas y dinámicas [SAST/DAST], análisis de interfaces de programación de aplicaciones [API], análisis de composición de software [SCA] y gestión de vulnerabilidades), los riesgos de la nube asociados a la configuración, los análisis de comportamientos en tiempo de ejecución y los requisitos de cumplimiento de normativas. Este cambio incrementa la necesidad de soluciones de seguridad nativas en la nube para proteger las plataformas nativas en la nube, en concreto contenedores/Kubernetes, hosts, dependencias de aplicaciones, códigos/aplicaciones serverless, herramientas CI/CD y otras plataformas de orquestación.

Fuente: Frost & Sullivan

Entorno de crecimiento (continuación)

En cuanto al consumo, las soluciones CSPM, CWPP y de seguridad de DevOps seguirán siendo funciones esenciales de CNAPP, pero los servicios de seguridad de red en la nube y CIEM también experimentarán un aumento en los próximos cinco años. Muchas organizaciones emplean al menos dos componentes del mismo proveedor al mismo tiempo, para mejorar la gestión y la eficiencia de la protección.

La consolidación de casos de uso de seguridad de la nube continuará en los próximos años. Se incorporarán más proveedores al espacio CNAPP, ya sea con sus propias tecnologías o a través de adquisiciones. Las empresas que tienen una oferta sólida de CWPP, como Kaspersky, Fortinet y VMware, probablemente entren en el mercado a través de una ampliación o adquisición de tecnología. Sin embargo, es posible que la mayor parte de la innovación en el desarrollo y la competencia venga de las start-ups que aportarán sus propias soluciones de seguridad nativas en la nube centradas en CSPM, CWPP y seguridad de DevOps.

Estudios de Frost & Sullivan relacionados con este análisis independiente:

- [Global Cloud Workload Protection \(CWP\) Growth Opportunities](#)
- [Global Cloud-native Application Protection Platform Growth Opportunities, 2022](#)

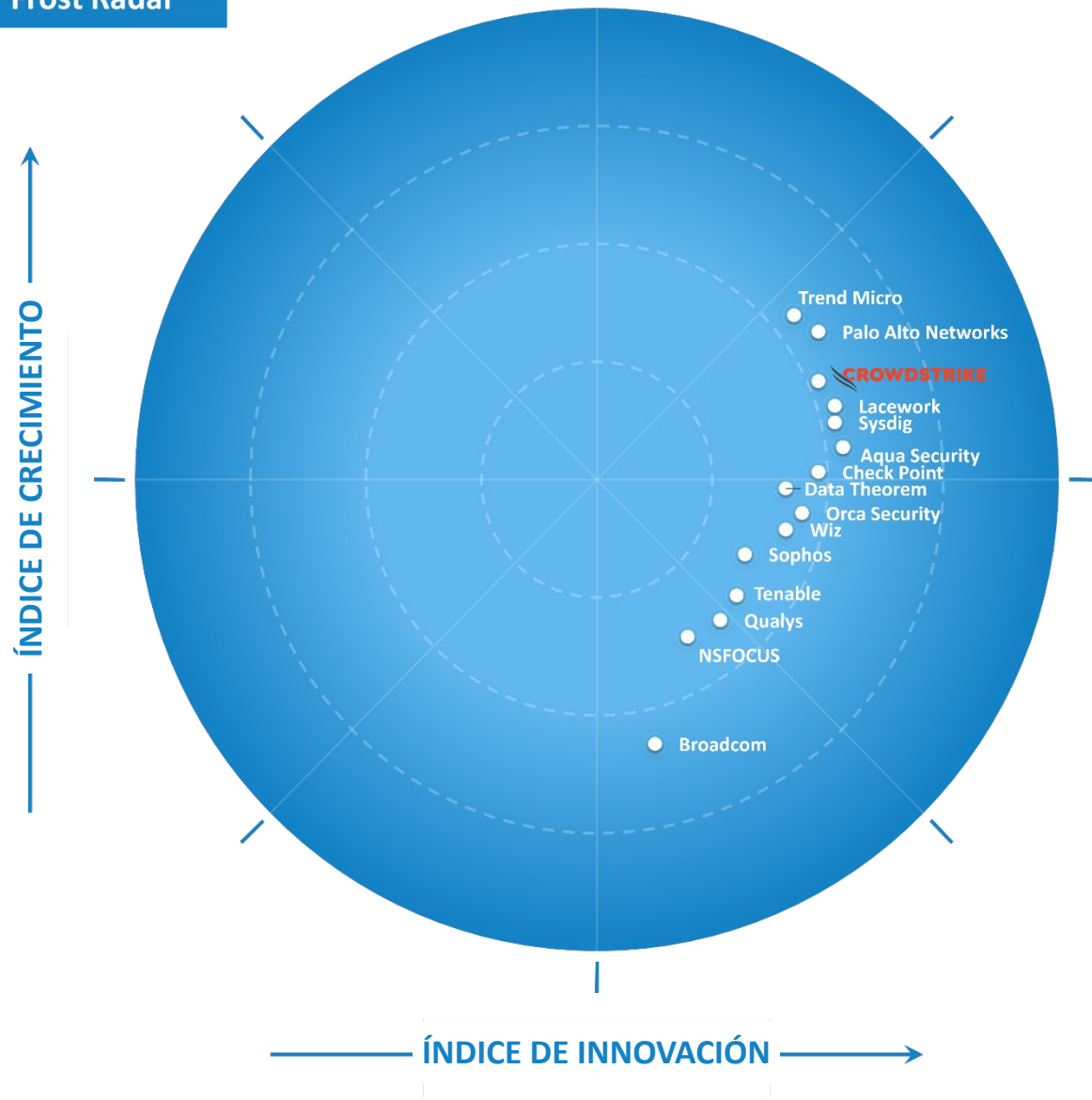


Frost Radar™

Plataformas de
protección de
aplicaciones nativas
en la nube

Frost Radar™: Plataformas de protección de aplicaciones nativas en la nube

Frost Radar™



Fuente: Frost & Sullivan

Frost Radar™

Entorno competitivo

El mercado de CNAPP sigue siendo relativamente incipiente y está muy fragmentado, con la participación de proveedores tradicionales de seguridad de endpoints y de red, proveedores de evaluación de vulnerabilidades y start-ups especializadas en seguridad de la nube. A partir de más de 20 participantes del sector procedentes de todo el mundo, Frost & Sullivan ha identificado de manera imparcial en este análisis Frost Radar™ a las 15 principales empresas. Los proveedores incluidos en el informe cumplen los siguientes criterios:

- presencia en al menos dos regiones (Norteamérica, Europa, Oriente Medio y África [EMEA], Asia-Pacífico [APAC] o Latinoamérica) en 2021 y en la primera mitad de 2022;
- ingresos anuales mínimos de 20 millones de dólares en 2021 y, como mínimo, un 1 % de cuota de mercado; y
- una plataforma CNAPP considerada idónea en septiembre de 2022 (es decir, una plataforma que incluya al menos funciones CSPM y CWPP).

Este informe de Frost Radar™ destaca las empresas siguientes: Aqua Security, Broadcom, Check Point Software Technologies, CrowdStrike, Data Theorem, Lacework, NSFOCUS, Orca Security, Palo Alto Networks, Qualys, Sophos, Sysdig, Tenable, Trend Micro y Wiz. Hay otras empresas que están explorando el mercado o que acaban de acceder a él, pero Frost & Sullivan identificó a estas como el motor que domina y conforma el mercado de CNAPP.

A medida que evolucione el mercado, se irán incorporando otras grandes empresas de ciberseguridad y start-ups de seguridad de la nube. Frost & Sullivan considera que el mercado será incluso más competitivo y que el panorama cambiará considerablemente en los próximos años, tanto en cuanto a estrategias de lanzamiento como en innovación tecnológica.

Entorno competitivo (continuación)

La capacidad de un proveedor para proporcionar una plataforma integrada que consolide y unifique las funciones de seguridad para ayudar a las empresas a gestionar su postura de seguridad y a detectar y responder a los riesgos a lo largo de todo el ciclo de vida de desarrollo de aplicaciones en el entorno nativo de la nube es el factor clave en el proceso de toma de decisiones de los clientes, junto con contar con opciones eficaces de soporte, el coste y un modelo de precios transparente y flexible.

Los clientes demandan un conjunto de funciones más amplio que les ofrezcan visibilidad y seguridad desde la creación hasta la producción y en infraestructuras de DevOps, DevSecOps y de la nube. Es decir, quieren soluciones CNAPP que cubran el espectro completo (código, aplicaciones, cargas de trabajo e infraestructuras). De hecho, estas soluciones pueden ayudarles a conseguir una estrategia de seguridad holística con una seguridad Zero Trust.

Las organizaciones emplean cada vez más la inteligencia artificial y el aprendizaje automático para gestionar mejor los riesgos en el entorno de nube. Por eso, la implementación de soluciones CNAPP tendrá realizarse antes (shift-left), en las primeras fases del diseño y el desarrollo del código, e integrarse con inteligencia artificial y aprendizaje automático para obtener mejor información del comportamiento de las cargas de trabajo y las aplicaciones, y de su interacción con la infraestructura de la nube, con el fin de mejorar la detección y la respuesta a las amenazas.

Aumenta la demanda de una integración más estrecha con la protección de aplicaciones web, motivada por la necesidad de que dicha protección converja con la de las cargas de trabajo de la nube subyacentes que las alimentan.

Entorno competitivo (continuación)

Si bien CNAPP está disponible con autoalojamiento y autogestión a través de un partner proveedor de servicios de seguridad gestionados, o como software como servicio (SaaS), los clientes tienden a optar por un modelo basado en la nube que le permite reducir los gastos, redistribuir los recursos según sus necesidades e incrementar la fiabilidad. Eso suele ocurrir sobre todo en el caso de las pequeñas y medianas empresas. Sin embargo, cuando se trata de empresas más grandes y pertenecientes a sectores muy regulados, el modelo de autoalojamiento sigue siendo conveniente, debido a los requisitos de privacidad y cumplimiento de normativas propios de este tipo de empresas.

CrowdStrike fue seleccionada en el Índice de crecimiento de Frost & Sullivan, porque presenta un crecimiento fuerte y constante en los tres últimos años, a pesar de que solo ocupa el séptimo lugar en cuanto a cuota de mercado. Frost & Sullivan aprecia su sólida base de clientes y su mejor percepción de marca, así como la importancia que otorga a la seguridad de la nube, lo que sin duda le permitirá mantener la marcada tendencia de crecimiento de su CNAPP en los próximos dos o tres años.

Empresas a seguir:
empresas prioritarias para inversiones,
alianzas o análisis comparativos

CrowdStrike

INNOVACIÓN

- La oferta CNAPP de CrowdStrike se compone de Falcon Cloud Workload Protection con agente, Falcon Horizon (CSPM) sin agente, CIEM y la seguridad de contenedores que se amplía con un modelo de seguridad shift-left como parte de la plataforma global CrowdStrike Falcon.
- La plataforma emplea tecnologías de análisis de comportamientos para la detección de las amenazas sin malware y los ataques sin archivos, para ayudar a las empresas a detectar y prevenir los errores de configuración de la nube, garantizar el cumplimiento normativo y administrar y proteger los hosts, las máquinas virtuales, y las aplicaciones y contenedores/Kubernetes, mediante la identificación temprana de vulnerabilidades, la detección y respuesta a amenazas, la protección en tiempo de ejecución y el cumplimiento de normativas. Aunque se ofrecen en dos módulos independientes, estas funcionalidades se pueden proporcionar a través de CrowdStrike Falcon mediante una base de datos propietaria que reagrupa Threat Graph, Asset Graph e Intel Graph, recopilada a partir de todos los endpoints, cargas de trabajo en la nube, contenedores y otras fuentes de datos de telemetría.

CRECIMIENTO

- CrowdStrike es uno de los proveedores de seguridad de la nube de más rápido crecimiento, fundamentalmente impulsado por sus soluciones XDR/EDR y MDR. Su negocio de CNAPP gana popularidad a nivel mundial, debido a su fuerte apuesta por el mercado de la seguridad de la nube.
- Según el cálculo de Frost & Sullivan, en 2021 los ingresos por CNAPP de CrowdStrike registraron un incremento interanual del 71,7 % y se convirtió en uno de los proveedores líderes del mercado, con una cuota del 5 %.
- Aunque la mayor parte de su negocio se concentra en Norteamérica, experimentó un crecimiento interanual del 92,6 % en la región de EMEA y un 82,3 % en APAC.
- CrowdStrike, que es uno de los proveedores de soluciones nativas de la nube de seguridad de endpoints de más rápido crecimiento, con un potente ecosistema de partners de canal, vende productos de gama superior y complementarios de sus módulos de seguridad de la nube a grandes empresas de múltiples sectores, lo que le ayuda a continuar creciendo.

PERSPECTIVA DE FROST

- CrowdStrike ha ganado popularidad por su oferta de CNAPP, que ha experimentado un rápido crecimiento en todo el mundo en los dos últimos años.
- Frost & Sullivan reconoce esta tendencia de crecimiento basada en su embudo de ventas sostenible, una sólida base de clientes procedente de sus productos XDR/EDR y un consolidado ecosistema de partners de canal, que contribuirán al avance del negocio de CNAPP.
- En particular, la capacidad de ofrecer servicios de MDR y Cloud Threat Hunting se considera un factor diferenciador respecto a otros competidores, ya que ayuda a mejorar la confianza de los clientes y la experiencia de uso de las soluciones.
- Sin embargo, CrowdStrike debería diversificar los casos de uso para su solución CNAPP con otras funcionalidades, como CSPM y CIEM, en lugar de CWPP. Además, debería ampliar su oferta de CNAPP con funcionalidades para el análisis de vulnerabilidades del código, lo que supondría un paso para conseguir que la plataforma fuera más integral.

Fuente: Frost & Sullivan



Reflexiones estratégicas

Reflexiones estratégicas

1

A pesar de su juventud, el mercado de CNAPP es cada vez más competitivo y se prevé la entrada de más proveedores en los dos o tres próximos años. Esto supone una enorme responsabilidad y añade presión a los proveedores existentes, que se ven obligados a mantener su ventaja competitiva con innovaciones tecnológicas y modelos de precios. Este alto nivel de competencia exige un mayor esfuerzo de los participantes en actividades de I+D y fusiones y adquisiciones, con el fin de reforzar las funcionalidades de sus plataformas y ganar terreno, además de encontrar formas de reducir el coste total de propiedad, proporcionando al mismo tiempo un mejor soporte y una mejor experiencia a sus clientes.


2

La educación del mercado es importante para conseguir que triunfe el nuevo sector de CNAPP. Es imprescindible que los proveedores colaboren estrechamente con otros participantes del sector para mejorar entre las empresas globales la concienciación sobre la seguridad de la nube y sobre la importancia del concepto de CNAPP en la transición a la nube. El crecimiento de los proveedores está impulsado en gran medida por los programas para partners de canal. Por lo tanto, para ellos es vital contar con los partners de canal adecuados, que puedan ayudarles a mejorar la concienciación en el mercado, promocionar sus soluciones, captar el interés de los clientes y ofrecer soporte local para ganarse la confianza de los clientes y convertirse en su opción preferida.

3

La elección y compra de CNAPP no es una decisión que un CISO pueda tomar solo. CNAPP requiere una colaboración más estrecha entre los directivos, ya que afecta a diferentes equipos de desarrollo, seguridad y operaciones, cada uno de ellos con sus propias estrategias, preferencias e indicadores de rendimiento (KPI). La decisión debe tener en cuenta la opinión de los CIO, los jefes de desarrollo y los directivos de la empresa, ya que todos ellos comparten un objetivo común.

Fuente: Frost & Sullivan



**Pasos siguientes:
utilizar el análisis
Frost Radar™ para la
capacitación de los
principales
interesados**

Importancia de estar en el Frost Radar™

Las empresas representadas en el Frost Radar™ son líderes del sector en cuanto a crecimiento, innovación o ambos, y contribuyen a la evolución del sector.

POTENCIAL DE CRECIMIENTO

Su organización tiene un importante potencial de crecimiento en el futuro, lo que la convierte en una empresa a seguir.

MEJORES PRÁCTICAS

Su empresa está bien posicionada para cumplir las mejores prácticas de Growth Pipeline™ en su sector.

INTENSIDAD

Su organización es uno de los principales impulsores de la intensidad competitiva en el entorno de crecimiento.

VALOR PARA EL CLIENTE

Su organización ha demostrado la capacidad de mejorar considerablemente su propuesta de valor para el cliente.

POTENCIAL DE PARTNERS

Su organización es considerada por clientes, inversores, partners de la cadena de valor y futuros profesionales como un proveedor de valor importante.

Fuente: Frost & Sullivan

Frost Radar™: una herramienta valiosa para el equipo directivo encargado del crecimiento

IMPERATIVOS ESTRATÉGICOS

- Crecimiento cada vez más difícil de alcanzar.
- Nivel de competencia elevado.
- Necesidad de reforzar la colaboración, el trabajo en equipo y la movilidad.
- Complejidad creciente del entorno.

FINALIDAD DEL FROST RADAR™

- Promover un entorno de colaboración propicio para la aplicación de buenas prácticas en el conjunto del equipo directivo mediante las herramientas necesarias.
- Evaluar el potencial de crecimiento mediante la plataforma de medición disponible.
- Apoyar al CEO gracias a la herramienta Growth Pipeline™.

PASOS SIGUIENTES

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline Dialog™ con el equipo Frost**

Fuente: Frost & Sullivan

Frost Radar™: una herramienta valiosa para los inversores

IMPERATIVOS ESTRATÉGICOS

- Flujo de transacciones bajo y competencia alta.
- Diligencia debida entorpecida por la complejidad del sector.
- Administración ineficaz de la cartera.

FINALIDAD DEL FROST RADAR™

- Los inversores pueden centrarse en el potencial de crecimiento creando un sólido embudo de empresas a seguir, para llevar a cabo inversiones de gran potencial.
- Realizar verificaciones de diligencia debida para mejorar y acelerar el proceso de las transacciones.
- Obtener la máxima rentabilidad interna y garantizar el éxito a largo plazo para los accionistas.
- Comparar regularmente el rendimiento con mejores prácticas para una administración óptima de la cartera.

PASOS SIGUIENTES

- **Growth Pipeline Dialog™**
- **Taller sobre el universo de oportunidades**
- **Growth Pipeline Audit™ como diligencia debida obligatoria**

Fuente: Frost & Sullivan

Frost Radar™: una herramienta valiosa para los clientes

IMPERATIVOS ESTRATÉGICOS

- Complejidad creciente de las soluciones, que podría tener implicaciones a largo plazo.
- Confusión provocada por las soluciones que ofrecen los proveedores.
- Incertidumbre acentuada por la volatilidad de los proveedores.

FINALIDAD DEL FROST RADAR™

- Evaluar a potenciales proveedores e identificar a los partners que proporcionarán soluciones eficaces a largo plazo, gracias al marco de análisis disponible.
- Evaluar las soluciones más innovadoras y saber cómo responde a sus necesidades cada una de ellas.
- Disponer de una perspectiva a largo plazo sobre las alianzas con proveedores.

PASOS SIGUIENTES

- **Growth Pipeline Dialog™**
- **Growth Pipeline Diagnostic™**
- **Sistema de análisis comparativo Frost Radar™**

Fuente: Frost & Sullivan

Frost Radar™: una herramienta valiosa para el consejo de administración

IMPERATIVOS ESTRATÉGICOS

- Cada vez es más difícil crecer; los CEO necesitan ayuda.
- Necesidad de disponer de competencias específicas para comprender el entorno de crecimiento.
- Evolución de la cadena de valor del cliente.

FINALIDAD DEL FROST RADAR™

- Supervisar el éxito a largo plazo mediante un sistema de medición único.
- Proteger las inversiones de los accionistas mediante una plataforma de discusión que se centra en los problemas de base, los criterios de referencia y las mejores prácticas.
- Garantizar la calidad del liderazgo, del soporte y de la gobernanza de los CEO a fin de maximizar el potencial de crecimiento.

PASOS SIGUIENTES

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Fuente: Frost & Sullivan

Análisis Frost Radar™



Frost Radar™: análisis comparativo del potencial de crecimiento

2 índices principales, 10 componentes analíticos, 1 plataforma

EJE VERTICAL

Índice de crecimiento (IC) es una medida del rendimiento y la evolución del crecimiento de una empresa, junto con su capacidad para desarrollar y ejecutar una estrategia y una visión de crecimiento perfectamente alineadas; un sistema de embudo de crecimiento robusto, así como estrategias eficaces de ventas y marketing centradas en el mercado, la competencia y los usuarios finales.

COMPONENTES DEL ÍNDICE DE CRECIMIENTO

- **IC1: CUOTA DE MERCADO (3 ÚLTIMOS AÑOS)**
Comparativa de la cuota de mercado de la empresa con la de sus competidores en un sector concreto durante los tres años anteriores.
- **IC2: CRECIMIENTO DE LOS INGRESOS (3 ÚLTIMOS AÑOS)**
Examen del índice de crecimiento de ingresos de una empresa durante los tres años anteriores en el mercado, sector y categoría que constituyen el contexto para del informe Frost Radar™ concreto.
- **IC3: EMBUDO DE CRECIMIENTO**
Evaluación de la eficacia y la influencia del sistema de embudo de crecimiento de una empresa para captar, analizar y priorizar continuamente su universo de oportunidades de crecimiento.
- **IC4: VISIÓN Y ESTRATEGIA**
Evaluación de cómo se ajusta la estrategia de crecimiento de una empresa a su visión. ¿Son coherentes las inversiones que realiza la empresa en productos y mercados con la visión indicada?
- **IC5: VENTAS Y MARKETING**
Medida de la eficacia de los esfuerzos de ventas y marketing de una empresa para incrementar la demanda y alcanzar sus objetivos de crecimiento.

Frost Radar™: análisis comparativo del potencial de crecimiento

2 índices principales, 10 componentes analíticos, 1 plataforma

COMPONENTES DEL ÍNDICE DE INNOVACIÓN

EJE HORIZONTAL

Índice de innovación (II) es una medida de la capacidad de una empresa para desarrollar productos/servicios/soluciones (con una idea clara de las megatendencias perjudiciales) que se pueden aplicar a nivel global, pueden evolucionar y ampliarse a varios mercados, y responden a las necesidades cambiantes de los clientes.

- **II1: ESCALABILIDAD DE LA INNOVACIÓN**

Determina si las innovaciones de una organización son escalables a nivel global y se pueden aplicar tanto a mercados en desarrollo como maduros, así como a sectores adyacentes y no adyacentes.

- **II2: INVESTIGACIÓN Y DESARROLLO**

Medida de la eficacia de la estrategia de I+D de la empresa, según el tamaño de su inversión en I+D y la gestión del embudo de innovación.

- **II3: CATÁLOGO DE PRODUCTOS**

Análisis del catálogo de productos de una empresa, centrándose en la contribución relativa de los nuevos productos a los ingresos anuales.

- **II4: INFLUENCIA DE LAS MEGATENDENCIAS**

Evaluación de la capacidad de una empresa para aprovechar de manera proactiva las distintas oportunidades a largo plazo y los nuevos modelos empresariales, como base de su embudo de innovación. Para obtener más información sobre las megatendencias, haga clic [aquí](#).

- **II5: IDONEIDAD PARA EL CLIENTE**

Evalúa si los productos/servicios/soluciones de una empresa son adecuados para sus clientes actuales y potenciales, y cómo influye en su estrategia de innovación el cambio de necesidades de los clientes.



Apéndice

Lista de abreviaturas

CNAPP: Cloud-Native Application Protection Platform (Plataforma de protección de aplicaciones nativas en la nube)

DAST: Dynamic Application Security Testing (Prueba dinámica de la seguridad de aplicaciones)

IAST: Interactive Application Security Testing (Prueba interactiva de la seguridad de aplicaciones)

SAST: Static Application Security Testing (Prueba estática de la seguridad de aplicaciones)

CSPM: Cloud Security Posture Management (Gestión de la postura de seguridad de la nube)

CWPP: Cloud Workload Protection Platform (Plataforma de protección de cargas de trabajo en la nube)

IaC: Infrastructure as a Code (Infraestructura como código)

CIEM: Cloud Infrastructure Entitlement Management (Gestión de los derechos sobre la infraestructura de nube)

CI/CD: Continuous Integration / Continuous Delivery (Integración continua/entrega continua)

API: Application Program Interface (Interfaz de programación de aplicaciones)

SCA: Software Composition Analysis (Análisis de composición de software)

SBOM: Software Bill of Materials (Nomenclatura de materiales)

CNWS: Cloud Networks Security (Seguridad de redes en la nube)

WAAP: Web Application and API Protection (Protección de aplicaciones web y API)

Descargo de responsabilidad

Frost & Sullivan no es responsable de ninguna información incorrecta suministrada por empresas o usuarios. La información cuantitativa de mercado se basa principalmente en entrevistas y, por lo tanto, está sujeta a fluctuaciones. Los servicios de investigación de Frost & Sullivan se limitan a las publicaciones que contienen información de mercado valiosa, proporcionada por un grupo seleccionado de clientes. Los clientes aceptan, al realizar pedidos o descargas, que los servicios de investigación de Frost & Sullivan son para uso interno y no están destinados a publicación general ni divulgación a terceros. Ninguna parte de este servicio de investigación se puede otorgar, prestar, revender o mostrar a personas que no sean clientes, sin autorización por escrito. Asimismo, ninguna parte puede ser reproducida, almacenada en un sistema de recuperación ni transmitida en ningún formato ni por ningún medio —electrónico, mecánico, fotocopia, grabación o cualquier otro—, sin el permiso del editor.

Para obtener más información respecto al permiso, diríjase a: permission@frost.com

© 2022 Frost & Sullivan. Todos los derechos reservados. Este documento contiene información extremadamente confidencial y es propiedad exclusiva de Frost & Sullivan. Ninguna parte puede distribuirse, citarse, copiarse ni reproducirse de forma alguna, sin la aprobación expresa de Frost & Sullivan.