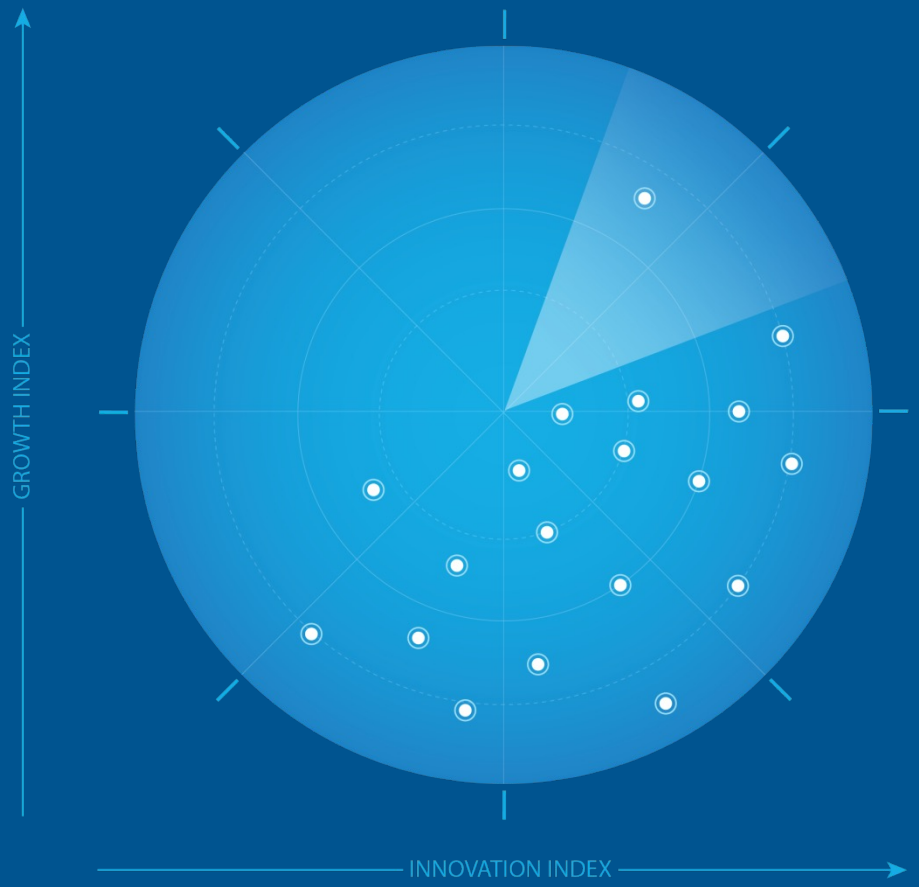
FROST & SULLIVAN

Frost Radar™: Plataformas de Protección de Aplicaciones Nativas en la Nube, 2022

Un sistema de análisis comparativo para impulsar a las empresas a la acción: innovación para impulsar el flujo de nuevos acuerdos y pipelines de crecimiento



Autor: Anh Tien Vu
Director de la industria, Ciberseguridad global

PD8C-74
Noviembre 2022

FROST & SULLIVAN

Imperativo Estratégico y Entorno de Crecimiento

Imperativo Estratégico

La informática en la nube se está convirtiendo en la norma en el entorno empresarial con una variedad de modelos y servicios disponibles en la nube. La migración acelerada a la nube ha permitido a las empresas empezar su recorrido de transformación digital y simplificar su infraestructura y operaciones de TI.

El uso de la informática en la nube está transformando el ciclo de vida de desarrollo de aplicaciones, las operaciones de seguridad y la forma en que las organizaciones construyen, operan y administran la infraestructura de back-end y aplicaciones de front-end, las aplicaciones orientadas al cliente con tecnologías nativas de la nube, como contenedores/Kubernetes, sin servidor, infraestructura como código (IaC, por sus siglas en inglés) y otras plataformas de integración/entrega continua (CI/CD, por sus siglas en inglés) para la administración, la aplicación, el desarrollo y la implementación en la nube.

Con un enfoque más intenso en las tecnologías de desarrollo de aplicaciones nativas de la nube, las organizaciones están cambiando de un modelo de desarrollo de aplicaciones monolíticas tradicionales a una arquitectura de microservicios y un enfoque en contenedores utilizando más dependencias y bibliotecas de código abierto.

Las tecnologías de contenedores/Kubernetes y la informática sin servidor están cambiando las estrategias de desarrollo de aplicaciones, ya que permiten que las organizaciones diseñen, desarrollen, prueben y desplieguen sus aplicaciones de manera flexible en el mercado, mejorando la experiencia del cliente. La encuesta anual de 2021 llevada a cabo por la Cloud Native Computing Foundation (CNCF) mostró que el 96 % de las organizaciones usa o evalúa Kubernetes y el 93 % usa actualmente, o planea usar, contenedores en la producción. Sin embargo, el uso de software de código abierto, bibliotecas/dependencias y registros ha introducido más amenazas y preocupaciones de seguridad porque estos artefactos de aplicaciones siguen estando en riesgo de vulnerabilidad en imágenes para contenedor, seguridad de host, inyección de código (para aplicaciones sin servidor) y problemas de cumplimiento.

Fuente: Frost & Sullivan

Imperativo Estratégico (continuación)

La creciente complejidad del entorno híbrido y de múltiples nubes, así como la creciente superficie de ataque y los desafíos de las operaciones de seguridad requieren una plataforma integrada y nativa de la nube para brindar a las organizaciones visibilidad, control y protección para las arquitecturas modernas de computación en la nube (p. ej., máquinas virtuales [VM], contenedores, Kubernetes, sin servidor) así como integrar la seguridad en el ciclo de vida del desarrollo de software y ayudar a las organizaciones a manejar los cumplimientos de manera efectiva. Esto hace que el enfoque de seguridad heredado quede obsoleto porque no está diseñado para admitir la microsegmentación o ser lo suficientemente sólido como para mantenerse al día con los cambios de la aplicación, particularmente en entornos de contenedores y sin servidor.

Como resultado, el CNCF ha pedido un cambio de paradigma a un modelo de seguridad "*shift-left and shield-right*" para proteger las aplicaciones nativas de la nube acercando la seguridad de workloads dinámicos que se identifican en función de atributos y metadatos, como etiquetas y tags. El modelo requiere que la seguridad se integre temprano y durante todo el ciclo de vida del desarrollo de la aplicación en lugar de solo en las fases posteriores, así como la gestión de la seguridad para el entorno de la nube en el que se implementan y ejecutan las aplicaciones, lo que impulsa la necesidad de una plataforma de protección de aplicaciones nativas en la nube (CNAPP).

Con la CNAPP, las organizaciones pueden hacer frente a estas amenazas y desafíos de seguridad con una plataforma de seguridad integrada en lugar de soluciones de seguridad puntuales, como la gestión de la postura de seguridad en la nube (CSPM, pos sus siglas en inglés), la plataforma de protección de workload en la nube (CWPP) o la gestión de vulnerabilidades. La CNAPP también permite una mejor colaboración entre los equipos de seguridad, TI/plataforma y desarrollo para mejorar la productividad y administrar los riesgos de manera más eficiente para sus entornos de nube.

Fuente: Frost & Sullivan

Entorno de Crecimiento

El mercado global de CNAPP registró ingresos de 1.720,6 millones de dólares en 2021, lo que representa un crecimiento interanual del 48,8 %. Frost & Sullivan proyecta que ese impulso continúe a una tasa de crecimiento anual compuesta del 25,7 % de 2021 a 2026, con ingresos que alcancen los $5.406,8 millones en 2026 debido a la creciente demanda de una plataforma de seguridad unificada que fortalezca la seguridad de la infraestructura en la nube y proteja las aplicaciones y los datos a lo largo de su ciclo de vida.

En general, las organizaciones han estado adoptando los componentes de CNAPP individualmente durante bastante tiempo, empezando con la CSPM para la visibilidad y el control de la seguridad en la nube y la CWPP para la protección y el cumplimiento en tiempo de ejecución. La inversión en seguridad de DevOps ha aumentado recientemente debido a la necesidad de seguridad de "*shift-left*" para inyectar seguridad en la etapa inicial del ciclo de vida de desarrollo de software. Del mismo modo, la gestión de derechos de infraestructura en la nube (CIEM, por sus siglas en inglés) y la seguridad de la red en la nube son de uso generalizado entre los primeros usuarios que utilizaron soluciones nativas de la nube de sus proveedores de servicios en la nube.

Dicho esto, las organizaciones de todo el mundo han estado invirtiendo significativamente en diferentes formas de CNAPP. La mayoría son para productos individuales que abordan casos de uso y desafíos específicos. El concepto de CNAPP, de consolidar todas estas herramientas, sigue siendo nuevo (al igual que el acrónimo), lo que genera cierta confusión entre los usuarios potenciales y un tratamiento cauteloso de los inversionistas. Sin embargo, la adopción acelerada de servicios en la nube y tecnologías de desarrollo de aplicaciones nativas de la nube junto con el aumento de la superficie de ataque en el entorno de la nube alentarán más inversiones en tecnologías de seguridad en la nube en general y en plataformas CNAPP en particular.

Fuente: Frost & Sullivan

Entorno de Crecimiento (continuación)

Muchas organizaciones, en particular las maduras, entienden que el riesgo de las aplicaciones en silos, el riesgo del código abierto y la incapacidad de responder rápidamente a las amenazas que enfrentan la infraestructura y los workloads pueden crear brechas de seguridad y complejidad para sus equipos. La necesidad de identificar, priorizar y remediar el riesgo de forma centralizada intensificará la demanda por CNAPP.

Se requiere una plataforma única que brinde una mejor protección de seguridad, visibilidad granular y eficiencia en la gestión de riesgos para administrar los riesgos de seguridad y cumplimiento en conjunto. Esto viene con la creciente aceptación de la estrategia de nubes múltiples, la necesidad continua de proteger workloads contra los ataques y la presión de centralizar la aplicación de políticas coherentes en diferentes entornos, ya sea infraestructura de nube, contenedores/Kubernetes, IaC o pipelines de CI/CD.

Existe una necesidad creciente de una mejor integración de CNAPP con la estructura del ciclo de vida de desarrollo de software, el DevOps, y las plataformas de pipeline de CI/CD para habilitar el enfoque de seguridad por diseño (método de seguridad *shift-left*) en cada etapa de la creación de software (desarrollo, pruebas, y despliegue). La integración de CNAPP con DevOps es para abordar las principales preocupaciones que giran en torno al escaneo de artefactos de aplicaciones (pruebas de seguridad de aplicaciones estáticas y dinámicas [SAST/DAST], escaneo de interfaz de programación de aplicaciones [API], análisis de composición de software [SCA] y gestión de vulnerabilidades), riesgos de la nube asociados con la configuración, análisis del comportamiento del tiempo de ejecución y requisitos de cumplimiento. El cambio está impulsando la necesidad de soluciones de seguridad para proteger las plataformas nativas de la nube, en particular contenedores/Kubernetes, hosts, dependencias de aplicaciones, aplicaciones/códigos sin servidor, herramientas de CI/CD y otras plataformas de orquestación.

Fuente: Frost & Sullivan

Entorno de Crecimiento (continuación)

En términos de consumo, CSPM, CWPP y la seguridad de DevOps siendo características clave de la CNAPP, pero la CIEM y los servicios de seguridad de red en la nube también verán una aceptación en los próximos 5 años. Muchas organizaciones parecen utilizar al menos dos componentes de un proveedor al mismo tiempo para mejorar la eficacia de la gestión y la protección.

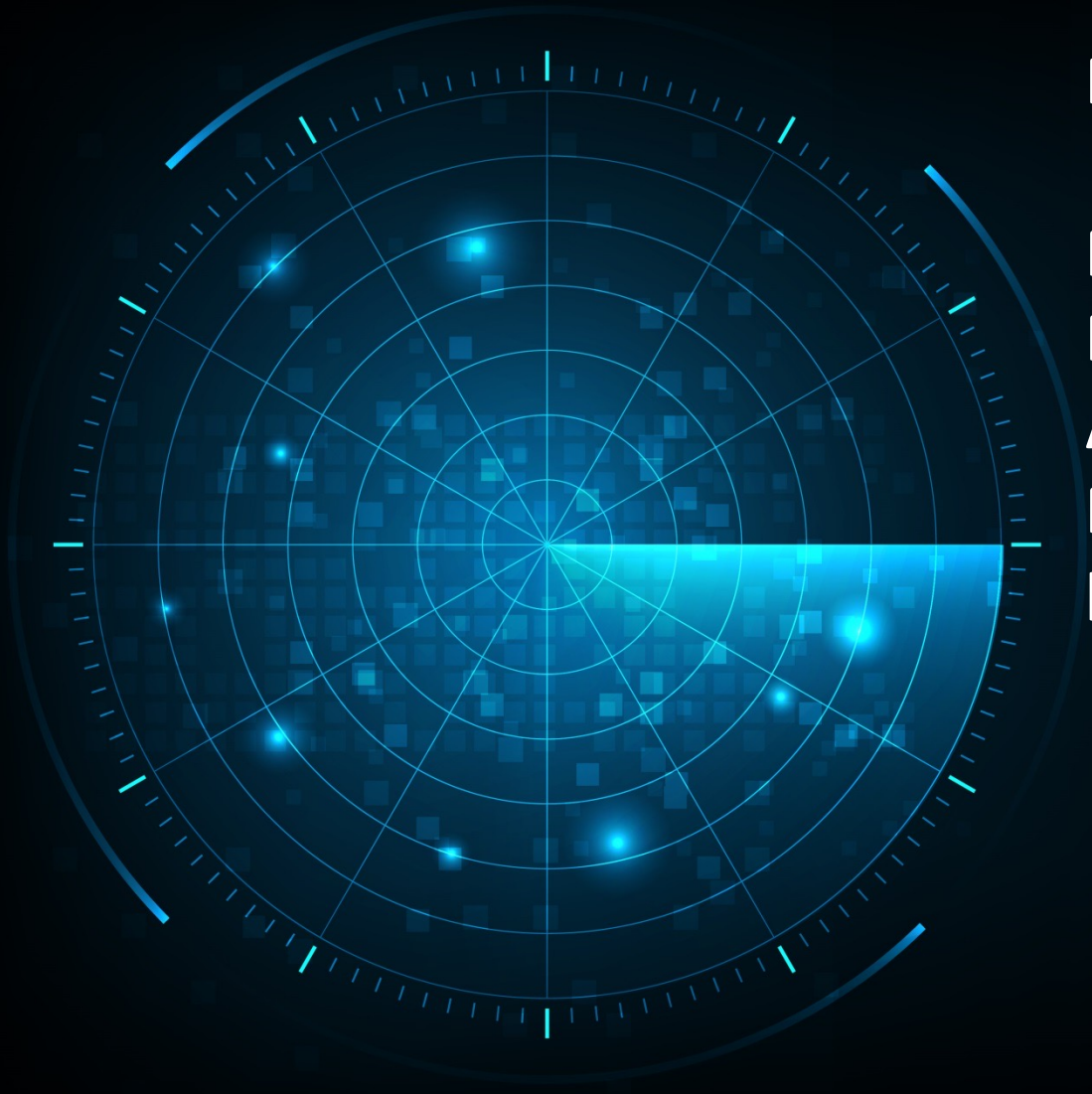
La consolidación de casos de uso de seguridad en la nube continuará en los próximos años. Más proveedores ingresarán al espacio CNAPP, ya sea con sus propias tecnologías patentadas o mediante adquisiciones. Las empresas que tienen ofertas sólidas de CWPP, incluidas Kaspersky, Fortinet y VMware, probablemente ingresarán al mercado a través de la expansión o adquisición de tecnología. No obstante, es probable que el mercado vea más desarrollo innovador y competencia de las nuevas empresas con sus propias soluciones de seguridad nativas de la nube que se centran en CSPM, CWPP y en la 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, 2022 Opportunities

Fuente: Frost & Sullivan

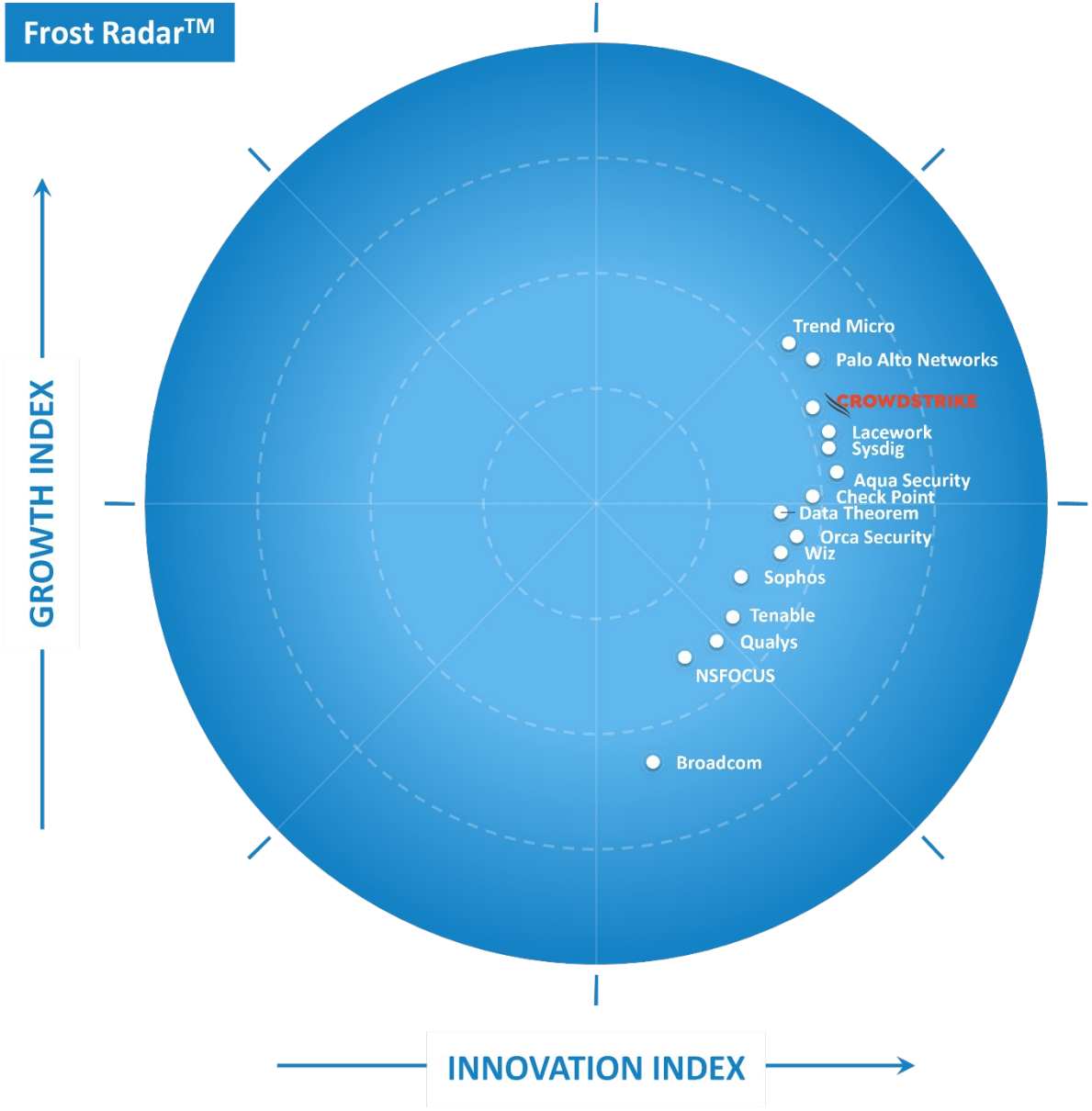
FROST & SULLIVAN



Frost Radar™:

Plataformas de Protección de Aplicaciones Nativas en la Nube

Frost Radar™: Plataformas de Protección de Aplicaciones Nativas en la Nube



Fuente: Frost & Sullivan

Frost Radar™

Entorno Competitivo

El mercado de CNAPP se mantuvo relativamente incipiente y fragmentado con la participación de proveedores tradicionales de seguridad de redes y terminales, proveedores de evaluación de vulnerabilidades y nuevas empresas que se especializan en seguridad en la nube. De un campo de más de 20 participantes de la industria a nivel mundial, Frost & Sullivan trazó de forma independiente las 15 principales empresas en este análisis Frost Radar™. Los proveedores incluidos en el informe cumplen con los siguientes criterios:

- presencia en al menos dos regiones (América del Norte; Europa, Oriente Medio y África [EMEA], Asia-Pacífico [APAC] o Latinoamérica) en 2021 y en la primera mitad de 2022;
- ingresos anuales de al menos $ 20 millones en 2021 y al menos una participación de mercado del 1%; y
- una plataforma CNAPP calificada para septiembre de 2022 (es decir, una plataforma que incluye al menos capacidades CSPM y CWPP).

Este Frost Radar™ cuenta con 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. Otras empresas están explorando o han ingresado en el mercado recientemente, pero Frost & Sullivan identificó las empresas mencionadas como las potencias que dominan y dan forma al mercado de CNAPP.

A medida que el mercado continúe evolucionando, ingresarán más grandes empresas de ciberseguridad y nuevas empresas de seguridad en la nube. Frost & Sullivan cree que el mercado se volverá aún más competitivo y que el panorama cambiará significativamente en los próximos años en términos de estrategias de comercialización e innovación tecnológica.

Fuente: Frost & Sullivan

Frost Radar™

Entorno Competitivo (continuación)

La capacidad de un proveedor para proporcionar una plataforma integrada que consolide y unifique las capacidades de seguridad para ayudar a las empresas a administrar la postura de seguridad y detectar y responder a los riesgos y amenazas de seguridad a lo largo del ciclo de vida del desarrollo de aplicaciones en el entorno nativo de la nube es el factor clave en el processo de toma de decisión de los clientes, junto con las sólidas capacidades de soporte, la asequibilidad y un modelo de precios flexible y transparente.

Los clientes buscan un conjunto más amplio de capacidades que puedan brindarles visibilidad y seguridad desde la construcción hasta la producción y en DevOps, DevSecOps e infraestructura en la nube. Esto significa que quieren soluciones CNAPP que cubran toda la pila (código, aplicación, workload e infraestructura). De hecho, estas soluciones pueden ayudarlos a lograr una estrategia de seguridad holística y alcanzar un estado de seguridad zero trust en diferentes entornos de nube.

Las organizaciones utilizan cada vez más las capacidades de inteligencia artificial/aprendizaje automático (IA/ML) para gestionar mejor los riesgos en el entorno de la nube. Como resultado, las soluciones de CNAPP tendrán que pasar a las primeras etapas de creación y desarrollo de código e integrarse con IA y ML para crear mejores conocimientos sobre el comportamiento del workload/aplicación y cómo interactúan dentro de la infraestructura de la nube para aumentar la automatización de la detección y respuesta a amenazas.

La demanda de una integración más sólida con la protección de aplicaciones web está aumentando debido a la necesidad de hacer converger dicha protección con los workloads de la nube subyacentes que las impulsan.

Fuente: Frost & Sullivan

Frost Radar™

Entorno Competitivo (continuación)

Si bien la CNAPP está disponible como autohospedada, administrada a través de una asociación de proveedores de servicios de seguridad administrados, o como software como servicio (SaaS), los clientes tienden a optar por un modelo de entrega en la nube para reducir los gastos generales, reasignar recursos y aumentar la confiabilidad. Esto es particularmente cierto para las pequeñas y medianas empresas. Sin embargo, para las grandes empresas y aquellas en industrias altamente reguladas, el modelo autohospedado seguirá siendo relevante debido a la necesidad de requisitos de privacidad y cumplimiento.

CrowdStrike fue elegida en el índice de crecimiento debido a su fuerte y constante crecimiento en los últimos tres años a pesar de que solo ocupa el séptimo lugar en términos de participación de mercado. Frost & Sullivan reconoce su sólida base de clientes y una mejor percepción de la marca, así como su importante enfoque en la seguridad en la nube, lo que seguramente le permitirá mantener un sólido impulso de crecimiento para su CNAPP en los próximos dos o tres años.

Fuente: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

Empresas a considerar primero para inversión, asociación o evaluación comparativa

CrowdStrike

INNOVACIÓN

- La oferta de CNAPP de CrowdStrike consiste en Falcon Cloud Workload Protection basado en agente, Falcon Horizon sin agente (CSPM), CIEM y seguridad de contenedores que se extiende a un modelo de seguridad *shift-left* como parte de la plataforma holística CrowdStrike Falcon.
- La plataforma utiliza tecnologías de análisis de comportamiento para la detección de amenazas sin malware y ataques sin archivos para ayudar a las empresas a detectar y prevenir configuraciones incorrectas de la nube, garantizar el cumplimiento y administrar y proteger hosts, máquinas virtuales, aplicaciones y contenedores/ Kubernetes a través de la identificación temprana de vulnerabilidades, detección de amenazas y respuesta, protección durante la ejecución y aplicación del cumplimiento. Aunque se ofrecen en dos módulos separados, estas capacidades se pueden entregar a través de CrowdStrike Falcon con la tecnología de una base de datos patentada Threat, Asset e Intel Graph recopilada de endpoints, workloads en la nube, contenedores y más fuentes de telemetría.

CRECIMIENTO

- CrowdStrike es uno de los proveedores de seguridad en la nube de más rápido crecimiento, impulsado principalmente por sus soluciones XDR/EDR y MDR. Su negocio CNAPP ha ganado terreno a nivel mundial porque el proveedor muestra un mayor enfoque en el mercado de seguridad en la nube.
- Según las estimaciones de Frost & Sullivan, los ingresos de CNAPP de CrowdStrike registraron un crecimiento interanual del 71,7 % en 2021 y se convirtió en uno de los proveedores líderes del mercado con una participación de mercado del 5 %.
- Aunque la mayoría de su negocio se encuentra en América del Norte, experimentó un crecimiento interanual del 92,6 % en EMEA y del 82,3 % en APAC.
- Como uno de los proveedores de seguridad de endpoints nativos en la nube de más rápido crecimiento con un sólido ecosistema de socios de canal, CrowdStrike puede realizar ventas cruzadas y aumentar las ventas de sus módulos de seguridad en la nube a grandes empresas en múltiples verticales, lo que le ayudará a mantener un fuerte impulso de crecimiento.

PERSPECTIVA FROST

- CrowdStrike ha ganado popularidad por su oferta de CNAPP a medida que creció rápidamente a nivel mundial en los últimos años.
- Frost & Sullivan reconoce su impulso de crecimiento a través de su cartera sostenible, su sólida base de clientes de XDR/EDR y su sólido ecosistema de socios de canal, que ayudarán a impulsar el negocio de CNAPP.
- En particular, la capacidad de proporcionar servicios de detección y respuesta gestionada (MDR) e investigación de amenazas en la nube se considera un punto de venta diferenciado en comparación con otros competidores, ya que puede ayudar a aumentar la confianza de los clientes y mejorar la experiencia cuando ellos usan las soluciones.
- No obstante, CrowdStrike debe diversificar los casos de uso de su solución CNAPP con otras capacidades, como CSPM, CIEM en lugar de CWPP. Además, debe expandir sus ofertas de CNAPP con capacidades para el escaneo de vulnerabilidades de código para hacer que su plataforma sea más completa.

Fuente: Frost & Sullivan

FROST & SULLIVAN

Perspectivas Estratégicas

Perspectivas Estratégicas

1

Aunque el mercado de CNAPP sigue siendo incipiente, se está volviendo cada vez más competitivo con la entrada de más proveedores en los próximos dos o tres años. Esto supondrá una gran responsabilidad y presión sobre los proveedores existentes para mantener sus ventajas competitivas tanto con las innovaciones tecnológicas como con los modelos de precios. La dura competencia requerirá que los participantes se esfuercen más en actividades de I+D y fusiones y adquisiciones para fortalecer las capacidades de su plataforma para ganar tracción y encontrar formas de reducir el costo total de propiedad, al mismo tiempo que pueden brindar un mejor.

2

La educación de mercado es importante para el éxito del mercado naciente de CNAPP. Es imperativo que los proveedores trabajen en estrecha colaboración con las partes interesadas de su industria para mejorar la conciencia sobre la seguridad en la nube entre las empresas globales y la importancia del concepto CNAPP en su recorrido en la nube. El crecimiento de los proveedores está impulsado en gran medida por sus programas de socios de canal. Como tal, es vital para los proveedores contar con socios de canal adecuados que puedan ayudar a educar al mercado, promover sus soluciones, interactuar con los clientes y brindar soporte local para ganar la confianza y la preferencia de los clientes.

3

La elección y compra de una CNAPP no es una decisión que un CISO pueda tomar solo. La CNAPP requiere una colaboración más estrecha en todos los ámbitos porque involucra varios equipos de desarrollo, seguridad y operaciones, cada uno con sus propias estrategias, preferencias e indicadores clave de rendimiento. La decisión debe incluir aportes de los directores de información, los desarrolladores principales y los líderes empresariales porque desean lograr un objetivo común.

Fuente: Frost & Sullivan

FROST & SULLIVAN

Próximos Pasos: Como usar Frost Radar™ para empoderar a las principales partes interesadas

Importancia de estar en el Frost Radar™

Las empresas analizadas en Frost Radar™ son líderes en la industria en cuanto a crecimiento, innovación o ambos. Son fundamentales para hacer avanzar la industria hacia el futuro.

POTENCIAL DE CRECIMIENTO

Su organización tiene un importante potencial de crecimiento futuro, lo que la convierte en una Company to Action.

MEJORES PRÁCTICAS

Su organización está bien posicionada para dar forma a las mejores prácticas de Growth Pipeline™ en su industria.

INTENSIDAD COMPETITIVA

Su organización es una de las impulsoras clave de la intensidad competitiva en el entorno de crecimiento.

VALOR PARA EL CLIENTE

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

POTENCIAL DE SOCIOS

Su organización es lo más importante para los clientes, inversores, socios de la cadena de valor y futuros talentos como proveedora de valor significativo.

Fuente: Frost & Sullivan

Frost Radar™ Empodera al Equipo de Crecimiento del CEO

IMPERATIVO ESTRATÉGICO

- El crecimiento es cada vez más difícil de lograr.
- La intensidad competitiva es alta.
- Se necesita más colaboración, trabajo en equipo y enfoque.
- El entorno de crecimiento es complejo.

APALANCANDO EL FROST RADAR™

- El equipo de crecimiento tiene las herramientas necesarias para fomentar un entorno de colaboración entre todo el equipo de gestión e impulsar las mejores prácticas.
- El equipo de crecimiento tiene una plataforma de medición para evaluar el potencial de crecimiento futuro.
- El equipo de crecimiento tiene la capacidad de apoyar al CEO con un poderoso Growth Pipeline™.

PRÓXIMOS PASSOS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Diálogo de Growth Pipeline™ con el Equipo Frost**

Fuente: Frost & Sullivan

Frost Radar™ Empodera a los Inversores

IMPERATIVO ESTRATÉGICO

- El flujo de negocios es bajo y la competencia es alta.
- La debida diligencia se ve obstaculizada por la complejidad de la industria.
- La gestión de cartera no es eficaz.

APALANCANDO EL FROST RADAR™

- Los inversores pueden enfocarse en el potencial de crecimiento futuro mediante la creación de un poderoso pipeline de Companies to Action para inversiones de alto potencial.
- Los inversores pueden realizar la diligencia debida que mejora la precisión y acelera el proceso de negociación.
- Los inversores pueden obtener la máxima tasa interna de rendimiento y garantizar el éxito de los accionistas a largo plazo
- Los inversores pueden comparar continuamente el rendimiento con las mejores prácticas para una gestión óptima de la cartera.

PRÓXIMOS PASSOS

- **Diálogo de Growth Pipeline™**
- **Taller Universo de Oportunidades**
- **Growth Pipeline Audit™ como diligencia debida obligatoria**

Fuente: Frost & Sullivan

Frost Radar™ Empodera a los Clientes

IMPERATIVO ESTRATÉGICO

- Las soluciones son cada vez más complejas y tienen implicaciones a largo plazo.
- Las soluciones de los proveedores pueden ser confusas.
- La volatilidad de los proveedores se suma a la incertidumbre.

APALANCANDO EL FROST RADAR™

- Los clientes tienen una estrutuctura analítica para evaluar a los proveedores potenciales e identificar a los socios que brindarán soluciones poderosas a largo plazo.
- Los clientes pueden evaluar las soluciones más innovadoras y comprender cómo las diferentes soluciones satisfarían sus necesidades.
- Los clientes obtienen una perspectiva a largo plazo sobre las asociaciones de proveedores.

PRÓXIMOS PASSOS

- **Diálogo de Growth Pipeline™**
- **Diagnóstico de Growth Pipeline™**
- **Sistema de evaluación comparativa Frost Radar™**

Fuente: Frost & Sullivan

Frost Radar™ empodera a la Junta Directiva

IMPERATIVO ESTRATÉGICO

- El crecimiento es cada vez más difícil; Los CEOs requieren orientación.
- El entorno de crecimiento requiere habilidades de navegación complejas.
- La cadena de valor del cliente está cambiando.

APALANCANDO EL FROST RADAR™

- La Junta Directiva tiene un sistema de medición único para garantizar la supervisión del éxito de la empresa a largo plazo.
- La Junta Directiva tiene una plataforma de discusión que se centra en los temas impulsores, los puntos de referencia y las mejores prácticas que protegerán la inversión de los accionistas.
- La Junta Directiva puede garantizar la tutoría, el apoyo y la gobernanza hábil del CEO para maximizar el potencial de crecimiento futuro.

PRÓXIMOS PASSOS

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

Fuente: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Analítica

Frost Radar™: Evaluación comparativa del potencial de crecimiento futuro

2 índices principales, 10 ingredientes analíticos, 1 plataforma

EJE VERTICAL

El **índice de crecimiento** (IC) es una medida del rendimiento e historial de crecimiento de una empresa, junto con su capacidad para desarrollar y ejecutar una estrategia y una visión de crecimiento totalmente alineadas; un sólido sistema de canalización de crecimiento; y estrategias eficaces de marketing y ventas centradas en el mercado, la competencia y el usuario final.

ELEMENTOS DEL ÍNDICE DE CRECIMIENTO

- **IC1: PARTICIPACIÓN DE MERCADO (3 AÑOS ANTERIORES)**
  Una comparación de la participación de mercado de una empresa en relación con sus competidores en un espacio de mercado determinado durante los 3 años anteriores.
- **IC2: CRECIMIENTO DE INGRESOS (3 AÑOS ANTERIORES)**
  Una mirada a la tasa de crecimiento de ingresos de una empresa durante los 3 años anteriores en el mercado/industria/categoría que forma el contexto para el Frost Radar™ dado.
- **IC3: PIPELINE DE CRECIMIENTO**
  Una evaluación de la fortaleza y el apalancamiento del sistema de línea de crecimiento de una empresa para capturar, analizar y priorizar continuamente su universo de oportunidades de crecimiento.
- **IC4: VISIÓN Y ESTRATEGIA**
  Una evaluación de qué tan bien la estrategia de crecimiento de una empresa está alineada con su visión. ¿Las inversiones que una empresa está haciendo en nuevos productos y mercados son consistentes con la visión declarada?
- **IC5: VENTAS Y MARKETING**
  Una medida de la eficacia de los esfuerzos de marketing y ventas de una empresa para ayudarla a impulsar la demanda y lograr sus objetivos de crecimiento.

Frost Radar™: Evaluación comparativa del potencial de crecimiento futuro

2 índices principales, 10 ingredientes analíticos, 1 plataforma

EJE HORIZONTAL

El **índice de innovación (II)** es una medida de la capacidad de una empresa para desarrollar productos/servicios/soluciones (con una comprensión clara de las megatendencias disruptivas) que son aplicables a nivel mundial, pueden evolucionar y expandirse para servir a múltiples mercados y están alineados con las necesidades cambiantes de los clientes.

ELEMENTOS DEL ÍNDICE DE INNOVACIÓN

- **II1: ESCALABILIDAD DE LA INNOVACIÓN**
  Esto determina si las innovaciones de una organización son globalmente escalables y aplicables tanto en mercados maduros como en desarrollo, y también en industrias verticales adyacentes y no adyacentes.
- **II2: INVESTIGACIÓN Y DESARROLLO**
  Esta es una medida de la eficacia de la estrategia de I+D de una empresa, determinada por el tamaño de su inversión en I+D y cómo ella alimenta la línea de innovación.
- **II3: CARTERA DE PRODUCTOS**
  Esta es una medida de la cartera de productos de una empresa, que se centra en la contribución relativa de los nuevos productos a sus ingresos anuales.
- **II4: USO DE LAS MEGA TENDENCIAS**
  Esta es una evaluación del uso proactivo de una empresa de oportunidades en evolución a largo plazo y nuevos modelos de negocios, como la base de su línea de innovación. Aquí está una explicación de las megatendencias.
- **II5: ALINEACIÓN CON LOS CLIENTES**
  Esto evalúa la aplicabilidad de los productos/servicios/soluciones de una empresa a los clientes actuales y potenciales, así como también cómo su estrategia de innovación se ve influenciada por las necesidades cambiantes de los clientes.

Apéndice

Lista de Abreviaciones

CNAPP: Plataforma de protección de aplicaciones nativas en la nube
DAST: Prueba de seguridad de aplicaciones dinámicas
IAST: Pruebas de seguridad de aplicaciones interactivas
SAST: Pruebas de seguridad de aplicaciones estáticas
CSPM: Gestión de la postura de seguridad en la nube
CWPP: Plataforma de protección de workload en la nube
IaC: Infraestructura como código
CIEM: Gestión de derechos de infraestructura en la nube
CI/CD: Integración Continua / Entrega Continua
API: Interfaz del programa de aplicación
SCA: Análisis de composición de software
SBOM: Lista de materiales del software
CNWS: Seguridad de redes en la nube
WAAP: Protección de aplicaciones web y API

Fuente: Frost & Sullivan

Aviso Legal

Frost & Sullivan no se hace responsable de la información incorrecta suministrada por las empresas o los usuarios. La información cuantitativa del mercado se basa principalmente en entrevistas y, por lo tanto, está sujeta a fluctuaciones. Los servicios de investigación de Frost & Sullivan son publicaciones limitadas que contienen valiosa información de mercado proporcionada a un grupo selecto de clientes. Los clientes reconocen, al solicitar o descargar los servicios de investigación de Frost & Sullivan, que ellos son para uso interno y no para publicación general o divulgación a terceros. Ninguna parte de este servicio de investigación se puede dar, prestar, revender o divulgar a personas que no sean clientes sin permiso por escrito. Además, ninguna parte puede reproducirse, almacenarse en un sistema de recuperación o transmitirse de ninguna forma ni por ningún medio (electrónico, mecánico, fotocopiado, grabación u otros) sin el permiso del editor.

Para obtener información sobre permisos, escriba a: allow@frost.com

© 2022 Frost & Sullivan. Todos los derechos reservados. Este documento contiene información altamente confidencial y es propiedad exclusiva de Frost & Sullivan. No se puede distribuir, citar, copiar o reproducir de otro modo ninguna parte de este documento sin la aprobación por escrito de Frost & Sullivan.