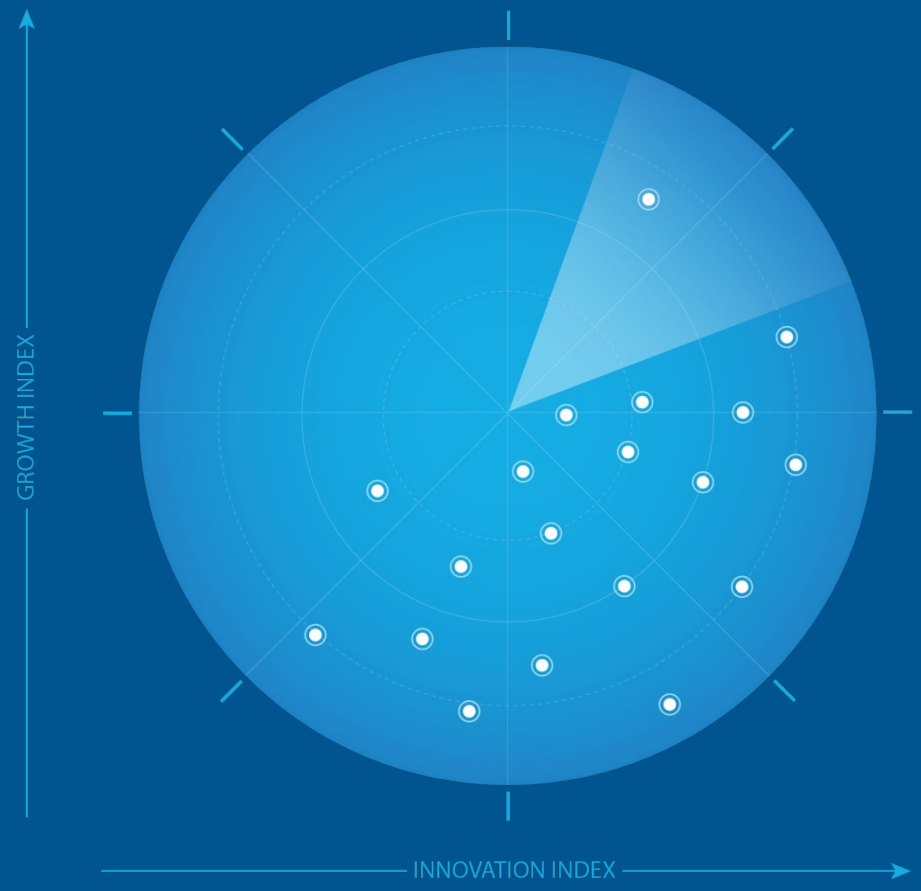
FROST & SULLIVAN

Frost Radar™: Plataformas de proteção de aplicações nativas em nuvem, 2022

Um sistema de benchmark para impulsionar empresas à ação - Inovação que alimenta fluxos de novos negócios e pipelines de crescimento



Autor: Anh Tien Vu
Industry Principal, Global Cybersecurity

PD8C-74
Novembro de 2022

FROST & SULLIVAN

Imperativo Estratégico e Ambiente de Crescimento

Imperativo Estratégico

A computação em nuvem está se tornando a norma no ambiente de negócios, contando com uma variedade de modelos e serviços de nuvem à disposição. A migração acelerada para a nuvem permitiu que as empresas embarcassem em sua jornada de transformação digital e simplificassem suas infraestruturas e operações de TI.

O uso da computação em nuvem está transformando o ciclo de vida do desenvolvimento de aplicações, as operações de segurança e a maneira como as organizações constroem, operam e gerenciam infraestrutura de back-end e aplicações de front-end voltadas para o cliente com tecnologias nativas em nuvem, como containers/Kubernetes, sem servidor, infraestrutura como código (IaC) e outras plataformas de integração/entrega contínua (CI/CD) para gerenciamento, aplicação, desenvolvimento e implementação de nuvem.

Com um foco mais intenso nas tecnologias de desenvolvimento de aplicações nativas em nuvem, as organizações estão mudando de um modelo de desenvolvimento de aplicações monolítico e tradicional para uma arquitetura de microsserviços e uma abordagem em containers, usando mais bibliotecas e dependências de código aberto.

As tecnologias de container/Kubernetes e a computação sem servidor estão mudando as estratégias de desenvolvimento de aplicações, pois permitem que as organizações projetem, desenvolvam, testem e lancem suas aplicações no mercado de forma flexível, melhorando a experiência do cliente. A Pesquisa Anual de 2021 da Cloud Native Computing Foundation (CNCF) mostrou que 96% das organizações estão usando ou avaliando o Kubernetes e 93% estão usando ou planejando usar containers na produção. No entanto, o uso de bibliotecas/dependências, registros e software de código aberto traz mais ameaças e preocupações de segurança, porque esses artefatos de aplicações seguem correndo risco quanto à vulnerabilidade da imagem do container, segurança de host, injeção de código (para aplicações sem servidor) e questões de conformidade.

Fonte: Frost & Sullivan

Imperativo Estratégico (continuação)

A crescente complexidade do ambiente híbrido e multinuvem, assim como a expansão da superfície de ataque e os desafios das operações de segurança, exigem uma plataforma integrada e nativa em nuvem para fornecer às organizações visibilidade, controle e proteção para proteger as arquiteturas modernas de computação em nuvem (por ex., máquinas virtuais [VMs], containers, Kubernetes, sem servidor), além de integrar a segurança no ciclo de vida do desenvolvimento de software e auxiliar as organizações a lidar de forma efetiva com questões de conformidade. Isso torna a abordagem de segurança legada desatualizada, porque não foi projetada para oferecer suporte à microssegmentação ou para ser robusta o suficiente para acompanhar as mudanças das aplicações, principalmente em ambientes sem servidor e containers.

Devido a isso, a CNCF defende uma mudança de paradigma para um modelo de segurança "*shift-left e shield-right*" para proteger aplicações nativas em nuvem trazendo a segurança para mais perto dos workloads dinâmicos, que são identificados com base em atributos e metadados, como etiquetas e tags. O modelo exige que uma segurança integrada desde o início e durante todo o ciclo de desenvolvimento da aplicação, e não só em fases posteriores, além do gerenciamento de segurança para o ambiente de nuvem no qual as aplicações são implementadas e executadas, o que aumenta a necessidade de uma plataforma de proteção de aplicações nativas em nuvem (CNAPP, Cloud-Native Application Protection Platform).

Com uma CNAPP, as organizações conseguem enfrentar essas ameaças e desafios de segurança com uma plataforma de segurança integrada, em vez de soluções pontuais de segurança como Gerenciamento de Postura de Segurança em Nuvem (CSPM, Cloud Security Posture Management), Plataforma de Proteção de Workload em Nuvem (CWPP, Cloud Workload Protection Platform) ou gerenciamento de vulnerabilidades. A CNAPP também permite melhor colaboração entre as equipes de segurança, TI/plataforma e desenvolvimento, melhorando a produtividade e gerenciando riscos de forma mais eficiente em seus ambientes de nuvem.

Fonte: Frost & Sullivan

Ambiente de Crescimento

O mercado global de CNAPP registrou uma receita de US$ 1.720,6 milhões em 2021, representando um crescimento ano a ano de 48,8%. A Frost & Sullivan projeta que esse *momentum* continuará, a uma taxa de crescimento anual composta de 25,7% de 2021 a 2026, com a receita atingindo US$ 5.406,8 milhões em 2026 devido à crescente demanda por uma plataforma unificada de segurança em nuvem que fortaleça a segurança da infraestrutura na nuvem e proteja aplicações e dados ao longo de seu ciclo de vida.

As organizações, em geral, já vêm adotando componentes CNAPP de forma individual há algum tempo, encabeçados por CSPM para visibilidade e controle de segurança na nuvem, e CWPP para proteção e conformidade em tempo de execução. O investimento em segurança de DevOps aumentou recentemente devido à necessidade de uma segurança *shift-left,* para injetar proteção no estágio inicial do ciclo de vida do desenvolvimento de softwares. Da mesma forma, o Gerenciamento de Direitos da Infraestrutura em Nuvem (CIEM, Cloud Infrastructure Entitlement Management) e a segurança de rede em nuvem são amplamente utilizados pelos *early cloud adopters,* que usaram soluções nativas em nuvem de seus provedores de serviços de nuvem.

Dito isso, organizações de todo o mundo têm feito gastos significativos em diferentes formas de CNAPP. A maioria, em produtos isolados, para atender a casos de uso e desafios específicos. O conceito CNAPP de consolidar todas essas ferramentas ainda é novo (assim como o acrônimo), gerando certa confusão entre usuários potenciais e cautela na hora de investir. Ainda assim, a adoção acelerada de serviços em nuvem e tecnologias de desenvolvimento de aplicações nativas em nuvem, associada ao aumento da superfície de ataque nos ambientes em nuvem, motivarão mais gastos com tecnologias de segurança em nuvem no geral e, em particular, com plataformas CNAPP.

Fonte: Frost & Sullivan

Ambiente de Crescimento (continuação)

Muitas organizações, especialmente as mais maduras, entendem que o risco de aplicações isoladas, o risco do código aberto e a incapacidade de responder rapidamente às ameaças a infraestrutura e workloads podem gerar lacunas de segurança e maior complexidade para suas equipes. A necessidade de identificar, priorizar e remediar riscos em uma visão centralizada intensificará a demanda por CNAPPs.

É necessária uma única plataforma que ofereça melhor proteção, visibilidade granular e eficiência no gerenciamento de riscos para administrar os riscos de segurança e conformidade juntos. Isso vem acompanhado de uma crescente aceitação da estratégia de multinuvem, da necessidade contínua de proteger workloads contra ataques e da pressão para que políticas sejam aplicadas de forma centralizada e consistente em diferentes ambientes, seja infraestrutura de nuvem, containers/Kubernetes, IaC ou pipelines de CI/CD.

Há uma necessidade crescente de uma melhor integração da CNAPP com a o ciclo de vida de desenvolvimento de software do DevOps e plataformas de pipeline CI/CD, para permitir a abordagem de segurança por design (segurança *shift-left*) em todas as etapas da construção dos softwares (desenvolvimento, teste e lançamento). A integração da CNAPP com o DevOps visa abordar as principais preocupações relacionadas à verificação de artefatos de aplicações (teste de segurança de aplicativo estático e dinâmico [SAST/DAST], verificação de Interface de Programação de Aplicação [API], análise de composição de software [SCA] e gerenciamento de vulnerabilidades), riscos da nuvem associados à configuração, análise de comportamento em tempo de execução e requisitos de conformidade. A mudança está impulsionando a necessidade por soluções de segurança nativas em nuvem para proteger plataformas nativas em nuvem, particularmente containers/Kubernetes, hosts, dependências de aplicações, aplicações/códigos sem servidor, ferramentas de CI/CD e outras plataformas de orquestração.

Fonte: Frost & Sullivan

Ambiente de Crescimento (continuação)

Em termos de consumo, CSPM, CWPP e a segurança de DevOps continuarão sendo recursos chave da CNAPP, mas CIEM e serviços de segurança de rede em nuvem também terão aceitação nos próximos cinco anos. Muitas organizações parecem usar pelo menos dois componentes de um fornecedor ao mesmo tempo, para melhorar o gerenciamento e a eficiência da proteção.

Casos de uso de consolidação da segurança em nuvem seguirão nos próximos anos. Mais fornecedores entrarão no espaço CNAPP com suas próprias tecnologias patenteadas ou através de aquisições. Empresas com ofertas fortes de CWPP, incluindo Kaspersky, Fortinet e VMware, provavelmente entrarão no mercado através de expansão ou aquisição de tecnologia. No entanto, é provável que o mercado veja mais concorrência e desenvolvimentos inovadores vindo de startups com suas próprias soluções de segurança nativas em nuvem focadas em CSPM, CWPP e na segurança de DevOps.

Estudos da Frost & Sullivan relacionados a esta análise independente:

- Global Cloud Workload Protection (CWP) Growth Opportunities
- Global Cloud-native Application Protection Platform Growth Opportunities, 2022

Fonte: Frost & Sullivan

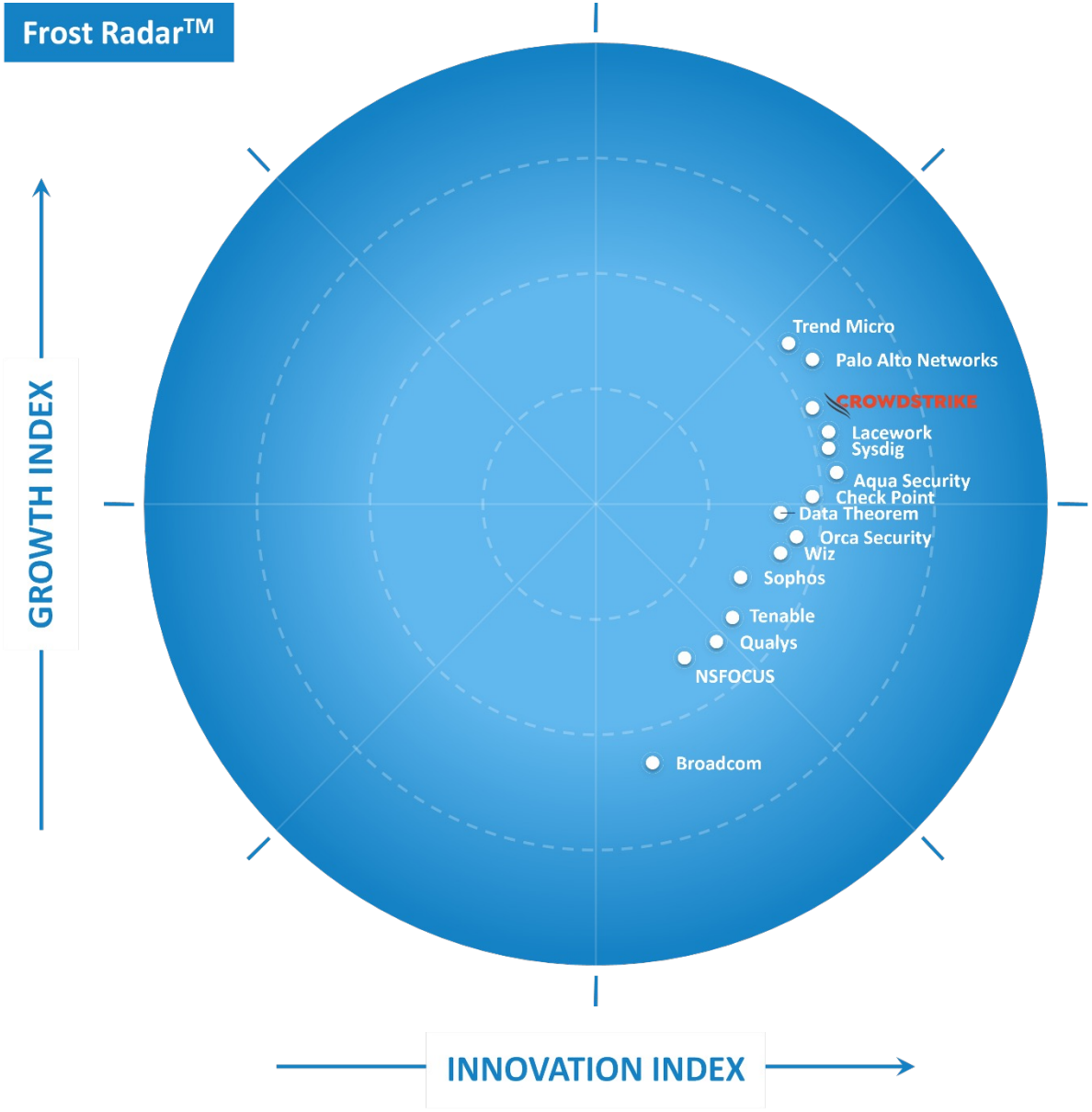
FROST & SULLIVAN

Frost Radar™

Plataformas de proteção de aplicações nativas em nuvem

Frost Radar™: Plataformas de proteção de aplicações nativas em nuvem

Frost Radar™



Fonte: Frost & Sullivan

Frost Radar™

Ambiente Competitivo

O mercado CNAPP permaneceu relativamente incipiente e fragmentado, com a participação de fornecedores tradicionais de segurança de rede e endpoint, fornecedores de avaliação de vulnerabilidade, e start-ups especializadas em segurança em nuvem. De um campo de mais de 20 participantes da indústria, de todo o mundo, a Frost & Sullivan analisou de forma independente as 15 principais empresas neste relatório do Frost Radar™. Os fornecedores incluídos no relatório atendem aos seguintes critérios:

- Presença em pelo menos duas regiões (América do Norte; Europa, Oriente Médio e África [EMEA], Ásia-Pacífico [APAC] ou América Latina) em 2021 e no primeiro semestre de 2022;
- Receita anual de pelo menos US$ 20 milhões em 2021 e pelo menos 1% de participação de mercado; e
- Uma plataforma CNAPP qualificada até setembro de 2022 (ou seja, uma plataforma que inclua pelo menos recursos de CSPM e CWPP).

Este Frost Radar™ analisou Aqua Security, Broadcom, Check Point Software Technologies, CrowdStrike, Data Theorem, Lacework, NSFOCUS, Orca Security, Palo Alto Networks, Qualys, Sophos, Sysdig, Tenable, Trend Micro e Wiz. Outras empresas estão explorando o mercado ou entraram nele recentemente, mas a Frost & Sullivan identificou os fornecedores acima como as potências que estão dominando e moldando o mercado de CNAPP.

À medida que o mercado continua a evoluir, mais empresas de grande porte de cibersegurança e start-ups de segurança em nuvem entrarão nele. A Frost & Sullivan acredita que o mercado se tornará ainda mais competitivo e que o cenário mudará significativamente nos próximos anos em termos de estratégias de entrada no mercado e inovação tecnológica.

Fonte: Frost & Sullivan

Frost Radar™

Ambiente Competitivo (continuação)

A capacidade de um fornecedor de oferecer uma plataforma integrada, que consolide e unifique os recursos de segurança para ajudar empresas a gerenciar a postura de segurança e detectar e responder a riscos e ameaças em todo o ciclo de desenvolvimento de aplicações em um ambiente nativo em nuvem é o principal fator na tomada de decisão dos clientes, junto com ter fortes recursos de suporte, custo acessível e um modelo de preços flexível e transparente.

Os clientes estão procurando por um conjunto mais amplo de recursos que forneça visibilidade e segurança desde a criação até a produção e abranja DevOps, DevSecOps e infraestrutura de nuvem. Isso significa que eles querem soluções CNAPP que cubram toda a pilha (código, aplicação, workload e infraestrutura). Essas soluções, de fato, podem ajudá-los a alcançar uma estratégia de segurança holística e atingir um estado de segurança zero-trust em diferentes ambientes de nuvem.

As organizações estão aproveitando cada vez mais os recursos de inteligência artificial/machine learning (AI/ML) para gerenciar melhor os riscos nos ambientes em nuvem. Como resultado, as soluções CNAPP terão que mudar para os estágios iniciais de criação e desenvolvimento do código e se integrar com IA e ML para criar melhores insights sobre o comportamento do workload/aplicação e como interagem na infraestrutura de nuvem para aumentar as capacidades automáticas de detecção e resposta de ameaças.

A demanda por uma integração mais forte com a proteção de aplicações web está aumentando devido à necessidade de convergir essa proteção com os workloads de nuvem subjacentes que as alimentam.

Fonte: Frost & Sullivan

Frost Radar™

Ambiente Competitivo (continuação)

Embora as CNAPPs estejam disponíveis como auto-hospedadas, administradas por parceria com provedor de serviços de segurança gerenciada, ou como SaaS (software como serviço), os clientes tendem a optar pelo modelo de entrega em nuvem para reduzir a sobrecarga, realocar recursos e aumentar a confiabilidade. Isto vale principalmente para pequenas e médias empresas. No entanto, para grandes empresas e setores altamente regulamentados, o modelo auto-hospedado permanecerá relevante devido aos requisitos de privacidade e conformidade.

A CrowdStrike foi apontada no Growth Index devido ao seu crescimento forte e consistente nos últimos três anos, apesar de ocupar apenas o sétimo lugar em termos de participação de mercado. A Frost & Sullivan reconhece sua forte base de clientes e melhor percepção da marca, assim como seu foco significativo em segurança de nuvem, o que certamente permitirá que mantenha o ritmo de crescimento robusto de sua CNAPP nos próximos dois a três anos.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

Empresas a considerar primeiro para investimentos, parcerias ou benchmarking

CrowdStrike

INOVAÇÃO

- A solução CNAPP da CrowdStrike consiste no Falcon Cloud Workload Protection baseado em agente, Falcon Horizon sem agente (CSPM), CIEM e segurança de container que se estende a um modelo de segurança *shift-left* como parte da plataforma holística CrowdStrike Falcon.
- A plataforma usa tecnologias de análise de comportamento para detecção de ameaças sem malware e ataques sem arquivo a fim de ajudar empresas a detectar e evitar configurações de nuvem incorretas, garantir a conformidade, gerenciar e proteger hosts, VMs, aplicações e containers/Kubernetes através da identificação antecipada de vulnerabilidades, detecção e resposta a ameaças, proteção de tempo de execução e cumprimento de conformidade. Embora oferecidos em 2 módulos separados, esses recursos podem ser fornecidos pelo CrowdStrike Falcon, alimentado pelo banco de dados patenteado Threat, Asset, and Intel Graph coletado de endpoints, workloads em nuvem, containers e outras fontes de telemetria.

CRESCIMENTO

- A CrowdStrike é um dos fornecedores de segurança em nuvem que mais cresce, impulsionada principalmente por suas soluções XDR/EDR e MDR. Sua CNAPP ganhou força globalmente porque a empresa mostra um foco mais forte no mercado de segurança em nuvem.
- Com base nas estimativas da Frost & Sullivan, a receita com CNAPP da CrowdStrike registrou um crescimento anual de 71,7% em 2021, o que a tornou um dos principais fornecedores do mercado, com market share de 5,0%.
- Embora a maioria de seus negócios esteja na América do Norte, a CrowdStrike teve um crescimento ano a ano de 92,6% na EMEA e de 82,3% na APAC.
- Sendo um dos vendors de segurança de endpoint nativos em nuvem que mais cresce e tendo um sólido ecossistema de parceiros de canal, a CrowdStrike pode fazer vendas cruzadas e upsell de seus módulos de segurança em nuvem para grandes empresas de vários setores, o que a ajudará a manter seu forte *momentum* de crescimento.

PERSPECTIVA FROST

- A CrowdStrike ganhou popularidade com sua solução CNAPP, pois cresceu rapidamente em nível global nos últimos dois anos.
- A Frost & Sullivan reconhece o ritmo de crescimento da CrowdStrike por seu pipeline sustentável, sua forte base de clientes, suas ofertas XDR/EDR e seu sólido ecossistema de parceiros de canal, que ajudarão a impulsionar a CNAPP no futuro.
- Em particular, a capacidade de fornecer serviços de detecção e resposta gerenciada (MDR) e investigação de ameaças na nuvem é vista como um argumento de vendas que destaca da concorrência, pois pode ajudar a aumentar a confiança dos clientes e melhorar a experiência de uso das soluções.
- Ainda assim, a CrowdStrike deve diversificar os casos de uso de sua solução CNAPP com outros recursos, como CSPM, CIEM em vez de CWPP. Além disso, deve expandir suas ofertas de CNAPP com recursos para varredura de vulnerabilidade de código, tornando sua plataforma mais abrangente.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Insights Estratégicos

Insights Estratégicos

1

Embora o mercado de CNAPPs permaneça incipiente, ele está se tornando cada vez mais competitivo com a entrada de mais fornecedores nos próximos dois a três anos. Isso colocará enorme ônus e pressão sobre os fornecedores existentes para manter suas vantagens competitivas com inovações tecnológicas e modelos de preços. A forte concorrência exigirá que os participantes se esforcem mais em atividades de P&D e M&A para fortalecer os recursos de suas plataformas a fim de ganhar tração e encontrar maneiras de reduzir o custo total de propriedade, enquanto ainda podem fornecer melhor suporte e experiências aos seus clientes.

2

A educação de mercado é importante para o sucesso do incipiente mercado de CNAPPs. É imperativo que os fornecedores trabalhem em estreita colaboração com as partes interessadas do setor para aumentar a conscientização sobre a segurança de nuvem entre as empresas globais e sobre a importância do conceito CNAPP em suas jornadas para a nuvem. O crescimento dos fornecedores é fortemente impulsionado por seus programas de parceiros de canal. Assim, é vital que os fornecedores tenham os parceiros de canal certos que possam ajudar a educar o mercado, promover suas soluções, interagir com os clientes e fornecer suporte local para ganhar a confiança e a preferência dos consumidores.

3

Escolher e adquirir uma CNAPP não é uma decisão que um CISO possa tomar sozinho. A CNAPP requer uma colaboração mais estreita entre todos os setores, porque envolve várias equipes de desenvolvimento, segurança e operações, cada uma com suas próprias estratégias, preferências e indicadores de desempenho. A decisão deve contar com a colaboração de CIOs (diretores de informações), desenvolvedores sênior e líderes de negócios, já todos estes desejam atingir um objetivo comum.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Próximos passos: Como usar o Frost Radar™ para empoderar os principais stakeholders

A importância de estar no Frost Radar™

As empresas que figuram no Frost Radar™ são líderes na indústria em termos de crescimento, inovação ou ambos. Elas são fundamentais para o avanço da indústria no futuro.

POTENCIAL DE CRESCIMENTO

Sua organização tem um potencial significativo de crescimento futuro, o que a torna uma Company to Action.

MELHORES PRÁTICAS

Sua organização está bem posicionada para moldar as melhores práticas do Growth Pipeline™ em seu setor.

INTENSIDADE COMPETITIVA

Sua organização é um dos principais impulsionadores da intensidade competitiva no ambiente de crescimento.

VALOR PARA O CLIENTE

Sua organização demonstrou a capacidade de aprimorar significativamente sua proposta de valor para o cliente.

POTENCIAL DE PARCEIRO

Sua organização é lembrada por clientes, investidores, parceiros da cadeia de valor e futuros talentos como uma forte provedora de valor.

Fonte: Frost & Sullivan

Frost Radar™ empodera a equipe de crescimento do CEO

IMPERATIVO ESTRATÉGICO

- Crescimento é algo cada vez mais difícil de alcançar.
- A intensidade competitiva é alta.
- Mais colaboração, trabalho em equipe e foco são necessários.
- O ambiente de crescimento é complexo.

COMO USAR O FROST RADAR™

- A equipe de crescimento possui as ferramentas necessárias para promover um ambiente colaborativo entre toda a gerência para impulsionar melhores práticas.
- A equipe de crescimento tem uma plataforma de medição para avaliar o potencial de crescimento futuro.
- A equipe de crescimento consegue apoiar o CEO com um poderoso Growth Pipeline™.

PRÓXIMOS PASSOS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Diálogo com Time Frost**

Fonte: Frost & Sullivan

Frost Radar™ empodera os investidores

IMPERATIVO ESTRATÉGICO

- O fluxo de negócios é baixo e a concorrência é alta.
- A devida diligência (due diligence) é prejudicada pela complexidade do setor.
- O gerenciamento de portfólio não é eficaz.

COMO USAR O FROST RADAR™

- Os investidores podem se concentrar no potencial de crescimento futuro ao criar um pipeline poderoso de Companies to Action para investimentos de alto potencial.
- Os investidores podem realizar a devida diligência, que melhora a precisão e acelera o processo de negociação.
- Os investidores podem obter taxa interna de retorno máxima e garantir o sucesso de longo prazo para os acionistas
- Os investidores podem avaliar continuamente o desempenho com as melhores práticas para otimizar o gerenciamento de portfólio.

PRÓXIMOS PASSOS

- **Diálogo Growth Pipeline™**
- **Workshop Universo de Oportunidades**
- **Growth Pipeline Audit™ como Devida Diligência Obrigatória**

Fonte: Frost & Sullivan

Frost Radar™ empodera os clientes

IMPERATIVO ESTRATÉGICO

- As soluções são cada vez mais complexas e têm implicações de longo prazo.
- As soluções dos fornecedores podem ser confusas.
- A volatilidade de fornecedores aumenta a incerteza.

COMO USAR O FROST RADAR™

- Os clientes têm uma estrutura analítica para avaliar fornecedores em potencial e identificar parceiros que fornecerão soluções poderosas e de longo prazo.
- Os clientes podem avaliar as soluções mais inovadoras e entender como diferentes soluções atenderiam às suas necessidades.
- Os clientes obtêm uma perspectiva de longo prazo quanto às parcerias com fornecedores.

PRÓXIMOS PASSOS

- **Diálogo Growth Pipeline™**
- **Diagnóstico Growth Pipeline™**
- **Sistema de Benchmarking Frost Radar™**

Fonte: Frost & Sullivan

Frost Radar™ empodera o conselho administrativo

IMPERATIVO ESTRATÉGICO

- O crescimento é cada vez mais difícil; os CEOs precisam de orientação.
- O ambiente de crescimento requer habilidades complexas para ser navegado.
- A cadeia de valor do cliente está mudando.

COMO USAR O FROST RADAR™

- O conselho administrativo ganha um sistema de medição exclusivo para garantir a supervisão do sucesso em longo prazo da empresa.
- O conselho administrativo tem uma plataforma de discussão centrada em problemas de impulsionamento, benchmarks e melhores práticas que protegerão o investimento dos acionistas.
- O conselho administrativo pode garantir uma orientação, apoio e governança qualificada do CEO para maximizar o potencial de crescimento futuro.

PRÓXIMOS PASSOS

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

Fonte: Frost & Sullivan

FROST & SULLIVAN

Análise Frost Radar™

Frost Radar™: Benchmarking do Potencial de Crescimento Futuro

2 Principais Índices, 10 Ingredientes Analíticos, 1 Plataforma

EIXO VERTICAL

O **Índice de Crescimento (IC)** é uma medida do desempenho e histórico de crescimento de uma empresa, aliado à sua capacidade de desenvolver e executar uma estratégia e visão de crescimento totalmente alinhadas; um sistema robusto de pipeline de crescimento; e estratégias eficazes de vendas e marketing focadas no mercado, na concorrência e no usuário final.

ELEMENTOS DO ÍNDICE DE CRESCIMENTO

- **IC1: PARTICIPAÇÃO DE MERCADO (3 ANOS ANTERIORES)**
  Uma comparação da participação de mercado da empresa em relação a seus concorrentes em um determinado espaço de mercado nos 3 últimos anos.
- **IC2: CRESCIMENTO DA RECEITA (3 ANOS ANTERIORES)**
  Uma visão da taxa de crescimento de receita da empresa nos 3 anos anteriores no mercado/indústria/categoria que forma o contexto para o Frost Radar™ em questão.
- **IC3: PIPELINE DE CRESCIMENTO**
  Uma avaliação da força e alavancagem do sistema de pipeline de crescimento da empresa para capturar, analisar e priorizar continuamente seu universo de oportunidades de crescimento.
- **IC4: VISÃO E ESTRATÉGIA**
  Esta é uma avaliação de quão bem a estratégia de crescimento da empresa está alinhada ã sua visão. Os investimentos que uma empresa está fazendo em novos produtos e mercados são consistentes com a visão declarada?
- **IC5: VENDAS E MARKETING**
  Esta é uma medida da eficácia dos esforços de vendas e marketing da empresa para ajudá-la a impulsionar a demanda e atingir seus objetivos de crescimento.

Frost Radar™: Benchmarking do Potencial de Crescimento Futuro

2 Principais Índices, 10 Ingredientes Analíticos, 1 Plataforma

ELEMENTOS DO ÍNDICE DE INOVAÇÃO

EIXO HORIZONTAL

O **Índice de Inovação (II)** é uma medida da capacidade de uma empresa de desenvolver produtos/serviços/soluções (com uma compreensão clara das Mega Tendências disruptivas) que sejam globalmente aplicáveis, capazes de evoluir e se expandir para atender a vários mercados, e estejam alinhados às necessidades em constante mudança dos clientes.

- **II1: ESCALABILIDADE DA INOVAÇÃO**
  Determina se as inovações da organização são globalmente escaláveis e aplicáveis tanto em mercados maduros quando nos em desenvolvimento e, também em indústrias verticais adjacentes e não adjacentes.
- **II2: PESQUISA E DESENVOLVIMENTO**
  Uma medida da eficácia da estratégia de P&D da empresa, determinada pelo volume de seu investimento em P&D e como ele alimenta o pipeline de inovação.
- **II3: PORTFÓLIO DE PRODUTOS**
  Medida do portfólio de produtos de uma empresa, com foco na contribuição relativa de novos produtos para sua receita anual.
- **II4: APROVEITAMENTO DE MEGA TENDÊNCIAS**
  Avaliação de como a empresa se beneficia proativamente de novos modelos de negócios e oportunidades em evolução de longo prazo como pilar de seu pipeline de inovação. Aqui temos uma explicação sobre Mega Tendências.
- **II5: ALINHAMENTO DO CLIENTE**
  Avalia a aplicabilidade dos produtos/serviços/soluções da empresa para clientes atuais e potenciais, e como sua estratégia de inovação é influenciada pela evolução das necessidades dos clientes.

Apêndice

Lista de Abreviações

CNAPP: Plataforma de proteção de aplicações nativas em nuvem
DAST: Teste de segurança de aplicativo dinâmico
IAST: Teste de segurança de aplicativo interativo
SAST: Teste de segurança de aplicativo estático
CSPM: Gerenciamento de postura de segurança em nuvem
CWPP: Plataforma de proteção de workload em nuvem
IaC: Infraestrutura como código
CIEM: Gerenciamento de direitos da infraestrutura de nuvem
CI/CD: Integração Contínua/Entrega Contínua
API: Interface de programação de aplicação
SCA: Análise de composição de software
SBOM: Lista de materiais de software
CNWS: Segurança de redes em nuvem
WAAP: Proteção de aplicações web e APIs

Fonte: Frost & Sullivan

Aviso Legal

A Frost & Sullivan não se responsabiliza por qualquer informação incorreta fornecida por empresas ou usuários. As informações quantitativas de mercado são baseadas principalmente em entrevistas e, portanto, estão sujeitas a flutuações. Os serviços de pesquisa da Frost & Sullivan são publicações limitadas contendo informações de mercado valiosas fornecidas a um grupo seleto de clientes. Os clientes reconhecem, ao fazer o pedido ou download, que os serviços de pesquisa da Frost & Sullivan são para uso interno e não para publicação geral ou divulgação a terceiros. Nenhuma parte deste serviço de pesquisa pode ser doada, emprestada, revendida ou divulgada a não clientes sem permissão por escrito. Além disso, nenhuma parte pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio - eletrônico, mecânico, fotocópia, gravação ou outro - sem a permissão da editora.

Para obter informações sobre tais permissão, escreva para: permission@frost.com