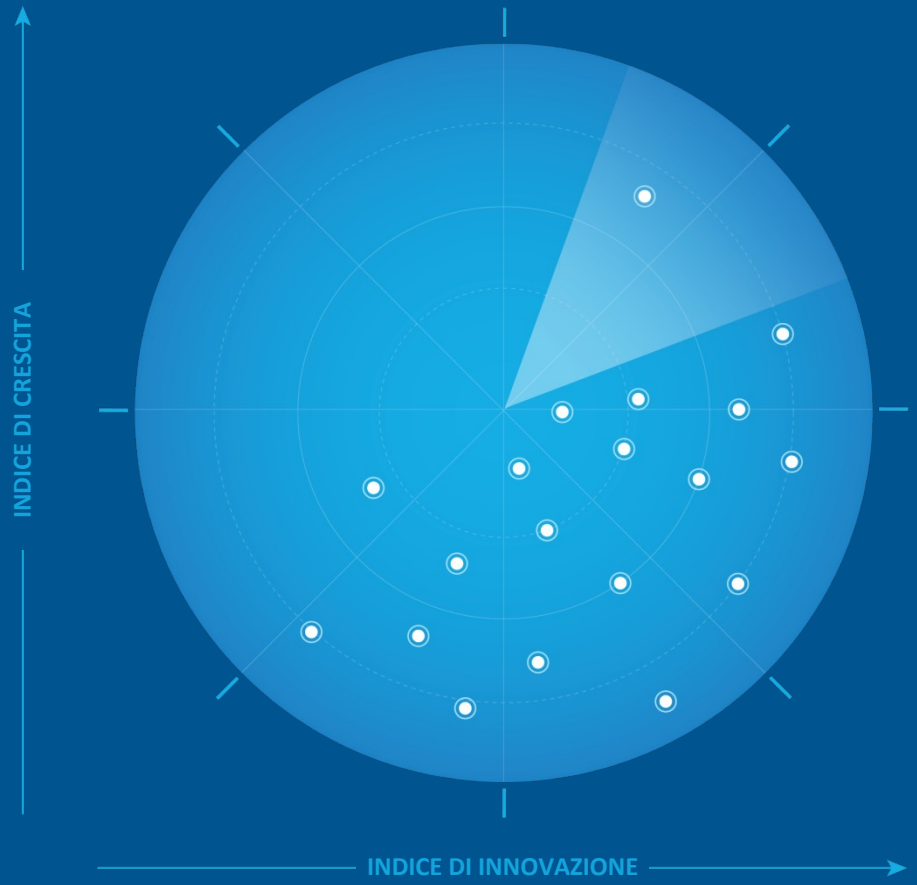
FROST & SULLIVAN

Frost Radar™: Cloud-Native Application Protection Platform, 2022

Un sistema di benchmarking per indurre le aziende all'azione: l'innovazione che alimenta il flusso di nuovi accordi e le pipeline di crescita



Autore: Anh Tien Vu
Direttore di settore, sicurezza informatica globale

PD8C-74
Novembre 2022

FROST & SULLIVAN

Imperativo strategico e ambiente di crescita

Imperativo strategico

Il cloud computing sta diventando la norma nell'ambiente aziendale, con un'ampia scelta di modelli e servizi cloud disponibili. La migrazione accelerata al cloud ha consentito alle aziende di intraprendere il percorso di trasformazione digitale e semplificare l'infrastruttura e le operazioni IT.

L'uso del cloud computing sta trasformando il ciclo di vita dello sviluppo delle applicazioni, le operazioni di sicurezza e il modo in cui le organizzazioni creano, azionano e gestiscono l'infrastruttura back-end e le applicazioni front-end rivolte ai clienti con tecnologie cloud native come container/Kubernetes, serverless, Infrastructure as Code (IaC) e altre piattaforme di integrazione continua/distribuzione continua (CI/CD) per la gestione, l'applicazione, lo sviluppo e la distribuzione del cloud.

Con una maggiore attenzione rivolta alle tecnologie di sviluppo delle applicazioni cloud native, le organizzazioni stanno passando da un tradizionale modello monolitico di sviluppo delle applicazioni a un'architettura di microservizi e un approccio containerizzato che utilizza più dipendenze e librerie open source.

Le tecnologie container/Kubernetes e l'elaborazione serverless stanno cambiando le strategie di sviluppo delle applicazioni poiché consentono alle organizzazioni di progettare, sviluppare, testare e lanciare in modo flessibile le proprie applicazioni sul mercato, migliorando così l'esperienza del cliente. L'indagine annuale 2021 della Cloud Native Computing Foundation (CNCF) ha rilevato che il 96% delle aziende sta utilizzando o valutando Kubernetes e che il 93% utilizza attualmente o prevede di utilizzare i container in produzione. Tuttavia, l'uso di software, librerie/dipendenze e registri open source ha introdotto un maggior numero di minacce e preoccupazioni per la sicurezza, poiché questi artefatti applicativi rimangono a rischio di vulnerabilità dell'immagine del container, di sicurezza dell'host, d'iniezione di codice (per applicazioni serverless) e di problemi di conformità.

Fonte: Frost & Sullivan

Imperativo strategico (segue)

La crescente complessità dell'ambiente ibrido e multi-cloud, nonché la superficie di attacco in espansione e le sfide delle operazioni di sicurezza, richiedono una piattaforma integrata e cloud native per fornire alle organizzazioni visibilità, controllo e protezione per proteggere le moderne architetture di cloud computing (ad es. macchine virtuali [VM], container, Kubernetes, serverless) e per integrare la sicurezza nel ciclo di vita dello sviluppo del software e consentire alle aziende di gestire efficacemente le conformità. Ciò rende l'approccio alla sicurezza legacy obsoleto perché non è stato concepito per supportare la micro-segmentazione o per essere abbastanza robusto da tenere il passo con le modifiche dell'applicazione, in particolare negli ambienti container e serverless.

Di conseguenza, il CNCF ha richiesto un cambio di paradigma verso un modello di sicurezza con "verifica precoce e attivazione della protezione" per proteggere le applicazioni cloud native avvicinando la sicurezza ai workload dinamici identificati in base ad attributi e metadati come etichette e tag. In base al modello, la sicurezza deve essere integrata fin dall'inizio e per tutto il ciclo di vita dello sviluppo dell'applicazione anziché solo nelle fasi successive, oltre alla gestione della sicurezza per l'ambiente cloud in cui le applicazioni sono distribuite e in esecuzione, il che determina la necessità di una piattaforma di protezione delle applicazioni cloud native (CNAPP).

Con CNAPP, le organizzazioni sono in grado di affrontare queste minacce e sfide alla sicurezza con una piattaforma di sicurezza integrata anziché affidarsi alle soluzioni di sicurezza mirate come la gestione dell'impostazione di sicurezza nel cloud (CSPM), la piattaforma di protezione dei workload cloud (CWPP) o la gestione delle vulnerabilità. CNAPP consente inoltre una migliore collaborazione tra i team di sicurezza, IT/piattaforma e sviluppo per migliorare la produttività e gestire i rischi in modo più efficiente per i propri ambienti cloud.

Fonte: Frost & Sullivan

Ambiente di crescita

Il mercato globale CNAPP ha registrato un fatturato di 1.720,6 milioni di dollari nel 2021, con una crescita del 48,8% rispetto all'anno precedente. La previsione di Frost & Sullivan è che questo slancio continui a un tasso di crescita annuo composto del 25,7% dal 2021 al 2026, con un fatturato che raggiungerà 5.406,8 milioni di dollari nel 2026 grazie alla crescente domanda di una piattaforma di sicurezza cloud unificata che rafforzi la sicurezza dell'infrastruttura cloud e protegga applicazioni e dati durante tutto il loro ciclo di vita.

L'adozione da parte delle organizzazioni di singoli componenti CNAPP è in atto da tempo, capeggiata da CSPM per la visibilità e il controllo della sicurezza del cloud e seguita da CWPP per la protezione e la conformità del runtime. Gli investimenti nella sicurezza DevOps sono aumentati di recente a causa della necessità di una sicurezza con verifica precoce per introdurre sicurezza nella fase iniziale del ciclo di vita dello sviluppo software. Analogamente, la gestione dei diritti dell'infrastruttura cloud (CIEM) e la sicurezza della rete cloud sono ampiamente utilizzate tra gli utenti precoci del cloud che hanno utilizzato soluzioni cloud native dei rispettivi fornitori di servizi cloud.

Detto questo, le organizzazioni di tutto il mondo hanno speso copiosamente per forme diverse di CNAPP. Per la maggior parte si tratta di singoli prodotti per risolvere casi d'uso e sfide specifici. Il concetto CNAPP del consolidamento di tutti questi strumenti rimane nuovo (così come l'acronimo), e genera una certa confusione tra i potenziali utenti e un approccio prudente agli investimenti. Tuttavia, l'adozione accelerata dei servizi cloud e le tecnologie di sviluppo di applicazioni cloud-native insieme all'aumento della superficie di attacco nell'ambiente cloud incoraggerà una maggiore spesa per le tecnologie di sicurezza cloud nel loro insieme e per le piattaforme CNAPP in particolare.

Fonte: Frost & Sullivan

Ambiente di crescita (segue)

Molte aziende, specie quelle mature, comprendono che il rischio delle applicazioni isolate, il rischio dell'open source e l'incapacità di rispondere rapidamente alle minacce che infrastruttura e workload devono fronteggiare, possono creare lacune di sicurezza e complessità per i loro team. La necessità di identificare, dare priorità e rimediare al rischio in una visione centralizzata non potrà che intensificare la domanda di CNAPP.

Per gestire contestualmente i rischi di sicurezza e conformità, è necessaria un'unica piattaforma che offra una migliore protezione della sicurezza, visibilità granulare ed efficienza nella gestione del rischio. Ciò deriva dalla crescente accettazione della strategia multi-cloud, dalla continua necessità di proteggere i workload dagli attacchi e dalla pressione per centralizzare l'applicazione uniforme delle policy in ambienti diversi, che si tratti di infrastrutture cloud, container/Kubernetes, IaC o pipeline CI/CD.

Esiste una necessità crescente nei confronti di una migliore integrazione di CNAPP con il framework del ciclo di vita dello sviluppo software DevOps e con le piattaforme di pipeline CI/CD per consentire l'approccio security-by-design (sicurezza con verifica precoce) in ogni fase della creazione del software (sviluppo, test e release). L'integrazione di CNAPP con DevOps serve a risolvere i problemi fondamentali che ruotano intorno alla scansione degli artefatti delle applicazioni (test di sicurezza delle applicazioni statiche e dinamiche [SAST/DAST], scansione dell'interfaccia di programmazione delle applicazioni [API], analisi della composizione del software [SCA] e gestione delle vulnerabilità), ai rischi del cloud associati alla configurazione, all'analisi del comportamento in fase di runtime e ai requisiti di conformità. Il passaggio sta determinando l'esigenza di soluzioni di sicurezza cloud native per proteggere le piattaforme native del cloud, in particolare container/Kubernetes, host, dipendenze delle applicazioni, applicazioni/codici serverless, strumenti CI/CD e altre piattaforme di orchestrazione.

Fonte: Frost & Sullivan

Ambiente di crescita (segue)

In termini di consumo, CSPM, CWPP e sicurezza DevOps continueranno a essere le caratteristiche fondamentali di CNAPP, ma anche CIEM e i servizi di sicurezza della rete cloud vedranno una diffusione nei prossimi 5 anni. Molte organizzazioni sembrano utilizzare almeno due componenti di un fornitore contemporaneamente per una migliore gestione ed efficienza di protezione.

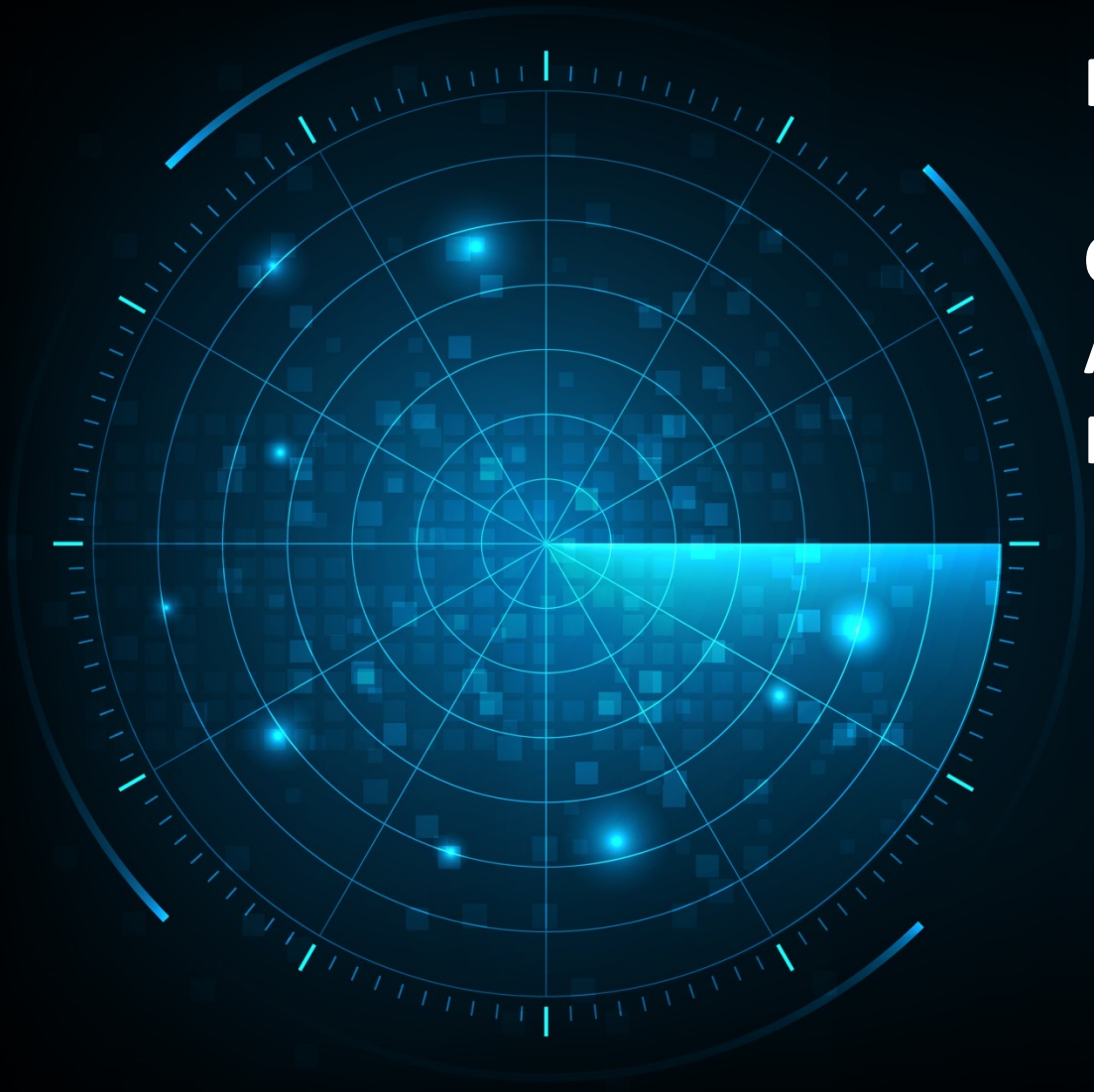
Il consolidamento dei casi d'uso della sicurezza cloud continuerà nei prossimi anni. Altri fornitori entreranno nello spazio CNAPP con le proprie tecnologie proprietarie o attraverso acquisizioni. Le aziende che vantano solide offerte CWPP, tra cui Kaspersky, Fortinet e VMware, molto probabilmente entreranno sul mercato attraverso l'espansione o l'acquisizione di tecnologia. Tuttavia, è probabile che il mercato veda uno sviluppo e una concorrenza a maggior contenuto innovativo da parte delle start-up e delle loro soluzioni di sicurezza cloud native incentrate sulla sicurezza CSPM, CWPP e DevOps.

Studi di Frost & Sullivan relativi a questa analisi indipendente:

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

Fonte: Frost & Sullivan

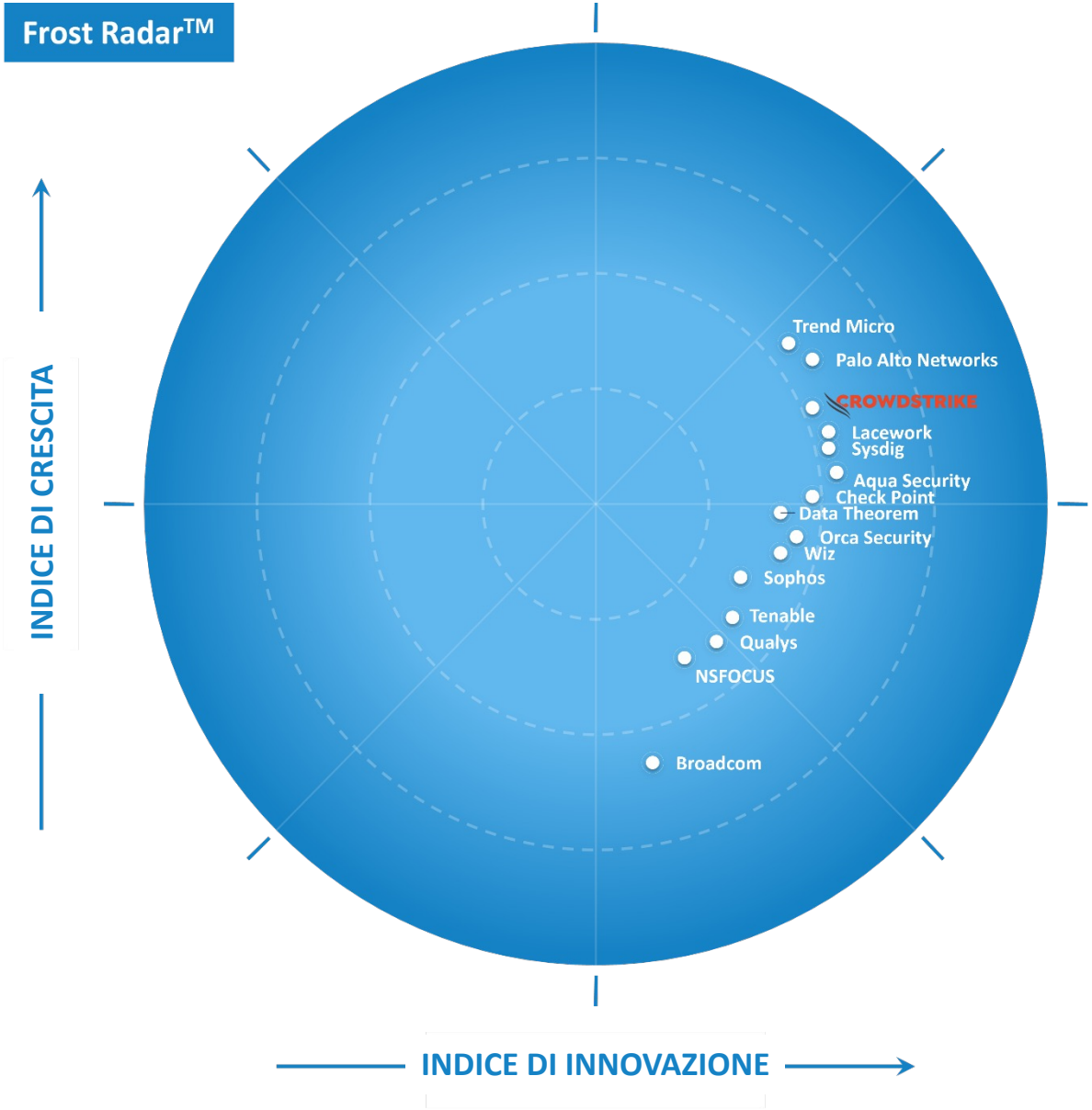
FROST & SULLIVAN



Frost Radar™

Cloud-Native Application Protection Platform

Frost Radar™: Cloud-Native Application Protection Platform



Fonte: Frost & Sullivan

Frost Radar™

Ambiente competitivo

Il mercato CNAPP è rimasto relativamente embrionale e frammentato con la partecipazione di fornitori tradizionali di sicurezza di reti ed endpoint, fornitori di valutazione delle vulnerabilità e start-up specializzate nella sicurezza cloud. Da un ambito di oltre 20 partecipanti di settore a livello globale, Frost & Sullivan ha rilevato in modo indipendente le prime 15 aziende in questa analisi Frost Radar™. I fornitori inclusi nel report soddisfano i seguenti criteri:

- presenza in almeno due regioni (Nord America; Europa, Medio Oriente e Africa [EMEA], Asia-Pacifico [APAC] o America Latina) nel 2021 e nella prima metà del 2022;
- entrate annuali di almeno 20 milioni USD nel 2021 e almeno una quota di mercato dell'1%;
- una piattaforma CNAPP qualificata entro settembre 2022 (ovvero una piattaforma che includa almeno funzionalità CSPM e CWPP).

Questo Frost Radar™ include 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. Altre aziende stanno esplorando il mercato o vi sono recentemente entrate, ma Frost & Sullivan le ha identificate come le potenze che stanno dominando e plasmando il mercato CNAPP.

Man mano che il mercato si evolve, un numero crescente di grandi società di sicurezza informatica e start-up di sicurezza cloud ne entrerà a far parte. Frost & Sullivan ritiene che il mercato diventerà ancora più competitivo e che il panorama cambierà sensibilmente nei prossimi due anni in termini sia di strategie go-to-market che di innovazione tecnologica.

Fonte: Frost & Sullivan

Frost Radar™

Ambiente competitivo (segue)

La capacità di un fornitore di approvvigionare una piattaforma integrata che consolidi e unifichi le funzionalità di sicurezza per agevolare l'azienda nella gestione dell'impostazione di sicurezza, e nel rilevare e rispondere ai rischi e alle minacce alla sicurezza, durante l'intero ciclo di vita dello sviluppo dell'applicazione nell'ambiente cloud native, è il fattore chiave del processo decisionale dei clienti, insieme alle solide capacità di supporto, alla convenienza e a un modello di prezzo flessibile e trasparente.

I clienti sono alla ricerca di una serie più ampia di funzionalità in grado di garantire loro visibilità e sicurezza dalla creazione alla produzione interessando DevOps, DevSecOps e infrastruttura cloud. Ciò significa che cercano soluzioni CNAPP che interessino tutta la gamma (codice, applicazione, workload e infrastruttura). Soluzioni che possono addirittura consentire loro di realizzare una strategia di sicurezza olistica e raggiungere uno stato di sicurezza zero-trust in diversi ambienti cloud.

Le organizzazioni sfruttano con sempre maggiore frequenza le capacità di intelligenza artificiale/machine learning (AI/ML) per gestire meglio i rischi nell'ambiente cloud. Le soluzioni CNAPP dovranno pertanto adottare la verifica precoce nelle fasi iniziali di ideazione e sviluppo del codice e integrarsi con AI e ML per creare migliori approfondimenti sul comportamento del workload/dell'applicazione e sulla sua interazione all'interno dell'infrastruttura cloud al fine di aumentare l'automazione delle capacità di rilevamento e risposta alle minacce.

La richiesta di una più solida integrazione con la protezione delle applicazioni web è in aumento a causa della necessità di far convergere tale protezione con quelle dei workload cloud sottostanti che le alimentano.

Fonte: Frost & Sullivan

Frost Radar™

Ambiente competitivo (segue)

Sebbene CNAPP sia disponibile in self-hosting, gestito tramite una partnership con un fornitore di servizi di sicurezza gestiti o come software as a service (SaaS), i clienti tendono a optare per un modello di distribuzione cloud per ridurre i costi di esercizio, ridistribuire le risorse e aumentare l'affidabilità. Ciò vale in particolar modo per le piccole e medie imprese. Per le grandi aziende e quelle in settori altamente regolamentati, invece, il modello in self-hosting resterà pertinente in ragione della necessità di privacy e dei requisiti conformità.

CrowdStrike è stata scelta nell'indice di crescita per la sua crescita solida e uniforme nel corso negli ultimi tre anni, malgrado si collochi solo al settimo posto in termini di quota di mercato. Frost & Sullivan riconosce il suo solido bacino clienti e la migliore percezione del brand, nonché la sua significativa attenzione alla sicurezza del cloud, che sicuramente consentirà a CrowdStrike di mantenere un forte slancio in crescita per il suo CNAPP nei prossimi due-tre anni.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Aziende in azione:

Aziende da considerare in prima battuta per investimenti, partnership o benchmarking

CrowdStrike

INNOVAZIONE

- L'offerta CNAPP di CrowdStrike è composta da Falcon Cloud Workload Protection agent-based, Falcon Horizon (CSPM) agentless, CIEM e sicurezza dei container che si estende a un modello di sicurezza con verifica precoce nell'ambito della piattaforma olistica CrowdStrike Falcon.
- La piattaforma utilizza tecnologie di analisi del comportamento per il rilevamento di minacce non malware e di attacchi "fileless" per consentire alle aziende di rilevare e prevenire configurazioni errate del cloud, garantire la conformità e gestire e proteggere host, macchine virtuali, applicazioni e container/Kubernetes attraverso l'identificazione precoce delle vulnerabilità, il rilevamento e la risposta alle minacce, la protezione del runtime e l'applicazione della conformità. Sebbene proposte in due moduli distinti, queste funzionalità possono essere distribuite tramite CrowdStrike Falcon alimentato da un database proprietario su minacce, risorse e a grafo raccolto da endpoint, workload cloud, container e altre fonti di telemetria.

CRESCITA

- CrowdStrike è uno dei fornitori di sicurezza cloud dalla crescita più rapida, spronata principalmente dalle sue soluzioni XDR/EDR e MDR. La sua attività CNAPP guadagnato seguito a livello globale perché il fornitore mostra una maggiore attenzione al mercato della sicurezza cloud.
- Sulla base delle stime di Frost & Sullivan, il fatturato CNAPP di CrowdStrike ha registrato una crescita del 71,7% nel 2021 rispetto all'anno precedente ed è diventato uno dei principali fornitori del mercato con una quota del 5,0%.
- Benché la sua attività sia principalmente dislocata in Nord America, ha registrato una crescita rispetto all'anno precedente del 92,6% in EMEA e dell'82,3% in APAC.
- Come uno dei fornitori di sicurezza cloud native per gli endpoint in più rapida crescita con un solido ecosistema di partner di canale, CrowdStrike può occuparsi di cross-selling e upselling dei propri moduli di sicurezza cloud a grandi aziende in più mercati verticali, il che consentirà all'azienda di mantenere un forte slancio di crescita.

PROSPETTIVA FROST

- CrowdStrike ha acquisito popolarità per la sua offerta CNAPP cresciuta rapidamente a livello globale negli ultimi due anni.
- Frost & Sullivan riconosce il suo slancio di crescita attraverso la sua pipeline sostenibile, un solido bacino clienti proveniente dalle sue offerte XDR/EDR e un consistente ecosistema di partner di canale, che contribuiranno a far progredire il business di CNAPP.
- In particolare, la capacità di fornire servizi MDR e di threat hunting è vista come un punto a favore differenziato rispetto ad altri concorrenti poiché può contribuire ad accrescere la fiducia dei clienti e a migliorare l'esperienza nell'utilizzo delle soluzioni.
- Tuttavia, CrowdStrike deve diversificare i casi d'uso per la sua soluzione CNAPP con altre funzionalità, come CSPM e CIEM anziché CWPP. Inoltre, deve ampliare la sua offerta CNAPP con funzionalità per la scansione delle vulnerabilità del codice, procedendo così a rendere la sua piattaforma più completa.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Approfondimenti strategici

Approfondimenti strategici

1

Anche se il mercato CNAPP resta embrionale, sta diventando sempre più competitivo grazie all'ingresso di altri fornitori nel corso dei prossimi due o tre anni. La conseguenza saranno un onere pesante e una forte pressione sui fornitori esistenti per mantenere i loro vantaggi competitivi sia con le innovazioni tecnologiche che con i modelli di prezzo. L'agguerrita concorrenza imporrà ai partecipanti di impegnarsi più efficacemente nelle attività di ricerca e sviluppo e di fusione e acquisizione, per potenziare le funzionalità della propria piattaforma, generare seguito e trovare modi per ridurre il costo totale di proprietà, pur restando in grado di fornire un supporto ed esperienze migliori ai propri clienti.

2

L'educazione al mercato è importante per il successo del nascente mercato CNAPP. È essenziale che i fornitori lavorino a stretto contatto con le parti interessate del settore per migliorare la consapevolezza della sicurezza cloud tra le aziende globali e l'importanza del concetto CNAPP nel loro viaggio verso il cloud.
La crescita dei fornitori è fortemente guidata dai loro programmi per i partner di canale. In tal senso, è essenziale che i fornitori dispongano dei giusti partner di canale in grado di aiutare a educare il mercato, promuovere le loro soluzioni, interagire con i clienti e fornire supporto locale per ottenere la fiducia e la preferenza dei clienti.

3

La scelta e l'acquisto di una piattaforma CNAPP non è una decisione che un CISO può prendere da solo.La CNAPP richiede una collaborazione più stretta su tutta la linea perché interessa vari team di sviluppo, sicurezza e operativi, ciascuno con le proprie strategie, preferenze e indicatori chiave di prestazione.La decisione deve includere il contributo di CFO, sviluppatori principali e leader aziendali perché desiderano tutti raggiungere un obiettivo comune.

Fonte: Frost & Sullivan

FROST & SULLIVAN

Passaggi successivi: Sfruttare Frost Radar™ per legittimare le principali parti interessate

Il significato di essere nel Frost Radar™

Le aziende tracciate su Frost Radar™ sono i leader del settore per crescita, innovazione o entrambi. Sono essenziali per propellere il settore nel futuro.

POTENZIALE DI CRESCITA

La tua organizzazione ha un potenziale di crescita futura significativo che la rende un'azienda in azione.

BEST PRACTICE

La tua organizzazione è ben posizionata per plasmare le best practice Growth Pipeline™ nel tuo settore.

INTENSITÀ COMPETITIVA

La tua organizzazione è uno dei fattori chiave dell'intensità competitiva nell'ambiente di crescita.

VALORE PER IL CLIENTE

La tua organizzazione ha dimostrato la capacità di migliorare sensibilmente la propria proposta di valore per il cliente.

POTENZIALE DI PARTNERSHIP

La tua organizzazione è la prima a cui si pensa per clienti, investitori, partner della catena del valore e futuri talenti in quanto fornitore di valore significativo.

Fonte: Frost & Sullivan

Frost Radar™ legittima il team di crescita del CEO

IMPERATIVO STRATEGICO

- Raggiungere la crescita è sempre più difficile.
- L'intensità competitiva è elevata.
- Servono maggiore collaborazione, lavoro di squadra e attenzione.
- L'ambiente di crescita è complesso.

SFRUTTARE FROST RADAR™

- Il team di crescita ha gli strumenti necessari per promuovere un ambiente collaborativo tra l'intero team di gestione al fine di orientare le best practice.
- Il team di crescita dispone di una piattaforma di misurazione per valutare il potenziale di crescita futuro.
- Il team di crescita ha la capacità di supportare il CEO con una potente Growth Pipeline™.

PASSAGGI SUCCESSIVI

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline Dialog™ e team Frost**

Fonte: Frost & Sullivan

Frost Radar™ legittima gli investitori

IMPERATIVO STRATEGICO

- Il flusso degli accordi è scarso e la concorrenza è alta.
- L'adeguata valutazione è ostacolata dalla complessità del settore.
- La gestione del portafoglio non è efficace.

SFRUTTARE FROST RADAR™

- Gli investitori possono concentrarsi sul potenziale di crescita futuro creando una potente pipeline di aziende in azione per investimenti ad alto potenziale.
- Gli investitori possono eseguire l'adeguata valutazione che migliora l'accuratezza e accelera il processo di negoziazione.
- Gli investitori possono realizzare il massimo tasso di rendimento interno e garantire il successo a lungo termine per gli azionisti.
- Gli investitori possono confrontare continuamente le prestazioni con le best practice per una gestione ottimale del portafoglio.

PASSAGGI SUCCESSIVI

- **Growth Pipeline Dialog™**
- **Laboratorio sull'universo delle opportunità**
- **Growth Pipeline Audit™ come adeguata valutazione obbligatoria**

Fonte: Frost & Sullivan

Frost Radar™ legittima i clienti

IMPERATIVO STRATEGICO	SFRUTTARE FROST RADAR™	PASSAGGI SUCCESSIVI
• Le soluzioni sono sempre più complesse e hanno implicazioni a lungo termine. • Le soluzioni dei fornitori possono confondere. • La volatilità dei fornitori accresce l'incertezza.	• I clienti dispongono di un quadro analitico per valutare i potenziali fornitori e identificare i partner capaci di fornire soluzioni potenti e a lungo termine. • I clienti possono valutare le soluzioni più innovative e capire come soluzioni diverse potrebbero soddisfare le loro esigenze. • I clienti acquisiscono una prospettiva a lungo termine sulle partnership con i fornitori.	• **Growth Pipeline Dialog™** • **Growth Pipeline Diagnostic™** • **Sistema di benchmarking Frost Radar™**

Fonte: Frost & Sullivan

Frost Radar™ legittima il consiglio d'amministrazione

IMPERATIVO STRATEGICO

- Raggiungere la crescita è sempre più difficile; ai CEO serve una guida.
- L'ambiente di crescita richiede abilità di navigazione complesse.
- La catena di valore del cliente sta cambiando.

SFRUTTARE FROST RADAR™

- Il Consiglio d'amministrazione dispone di un sistema di misurazione unico per garantire la supervisione del successo aziendale a lungo termine.
- Il Consiglio d'amministrazione dispone di una piattaforma di discussione incentrata su questioni determinanti, benchmark e best practice che proteggeranno gli investimenti degli azionisti.
- Il Consiglio d'amministrazione può garantire un tutoraggio, un supporto e una governance competenti del CEO per massimizzare il potenziale di crescita futuro.

PASSAGGI SUCCESSIVI

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

Fonte: Frost & Sullivan

FROST & SULLIVAN

Analisi di Frost Radar™

Frost Radar™: Riparametrazione del potenziale di crescita futura

2 indici principali, 10 ingredienti analitici, 1 piattaforma

ASSE VERTICALE

Indice di crescita (Growth Index, GI): è una misura delle prestazioni di crescita e dei precedenti di un'azienda, oltre alla sua capacità di sviluppare ed eseguire una strategia e una visione di crescita completamente allineate, un solido sistema di pipeline di crescita ed efficaci strategie di vendita e marketing mirate al mercato, alla concorrenza e all'utente finale.

ELEMENTI DELL'INDICE DI CRESCITA

- **GI1: QUOTA DI MERCATO (3 ANNI PRECEDENTI)**
  È un confronto della quota di mercato di un'azienda rispetto ai suoi concorrenti in un dato spazio di mercato per i 3 anni precedenti.
- **GI2: CRESCITA DEL FATTURATO (3 ANNI PRECEDENTI)**
  È uno sguardo al tasso di crescita del fatturato di un'azienda nei 3 anni precedenti nel mercato/settore/categoria che costituisce il contesto per il Frost Radar™ dato.
- **GI3: PIPELINE DI CRESCITA**
  Questa è una valutazione della forza e della leva del sistema di pipeline di crescita di un'azienda per acquisire, analizzare e assegnare continuamente la priorità al proprio universo di opportunità di crescita.
- **GI4: VISIONE E STRATEGIA**
  È una valutazione di quanto la strategia di crescita di un'azienda sia in linea con la sua visione. Gli investimenti di un'azienda in nuovi prodotti e mercati sono coerenti con la visione dichiarata?
- **GI5: VENDITE E MARKETING**
- È una misura dell'efficacia delle attività di vendita e marketing di un'azienda nel consentirle di orientare la domanda e raggiungere i propri obiettivi di crescita.

Frost Radar™: Riparametrazione del potenziale di crescita futura

2 indici principali, 10 ingredienti analitici, 1 piattaforma

ASSE ORIZZONTALE

Indice di innovazione (Innovation Index II) è una misura della capacità di un'azienda di sviluppare prodotti/servizi/soluzioni (con una chiara comprensione dei dirompenti megatrend) applicabili a livello globale, in grado di evolversi ed espandersi per servire più mercati e allineati alle mutevoli esigenze dei clienti.

ELEMENTI DELL'INDICE DI INNOVAZIONE

- **II1: INNOVATION SCALABILITY**
  Determina se le innovazioni di un'organizzazione sono scalabili a livello globale e applicabili sia nei mercati in via di sviluppo che in quelli maturi, e anche nei mercati verticali adiacenti e non.
- **II2: RICERCA E SVILUPPO**
  È una misura dell'efficacia della strategia di ricerca e sviluppo di un'azienda, determinata dalle dimensioni del suo investimento in ricerca e sviluppo e da come alimenta la pipeline dell'innovazione.
- **II3: PORTAFOGLIO PRODOTTI**
  È una misura del portafoglio prodotti di un'azienda, incentrata sul contributo relativo dei nuovi prodotti al rispettivo fatturato annuo.
- **II4: LEVA DEI MEGATREND**
  È una valutazione del modo proattivo in cui un'azienda mette a frutto le opportunità in evoluzione a lungo termine e nuovi modelli di business, come fondamento della propria pipeline di innovazione. Una descrizione del significato di megatrend è disponibile qui.
- **II5: ALLINEAMENTO CON IL CLIENTE**
  Valuta l'applicabilità dei prodotti/servizi/soluzioni di un'azienda ai clienti attuali e potenziali, nonché il modo in cui la sua strategia di innovazione è influenzata dall'evoluzione delle esigenze dei clienti.

Appendice

Elenco delle abbreviazioni

CNAPP: Cloud-Native Application Protection Platform (Piattaforma di protezione delle applicazioni cloud-native)

DAST: Dynamic Application Security Testing (Test dinamici di sicurezza delle applicazioni)

IAST: Interactive Application Security Testing (Test interattivi di sicurezza delle applicazioni)

SAST: Static Application Security Testing (Test statici di sicurezza delle applicazioni)

CSPM: Cloud Security Posture Management (Gestione dell'impostazione di sicurezza del cloud)

CWPP: Cloud Workload Protection Platform (Piattaforma di protezione dei workload cloud)

IaC: Infrastructure as Code (Infrastruttura come codice)

CIEM: Cloud Infrastructure Entitlement Management (Gestione dei diritti dell'infrastruttura cloud)

CI/CD: Continuous Integration / Continuous Delivery (Integrazione continua/distribuzione continua)

API: Application Program Interface (Interfaccia di programmazione di un'applicazione)

SCA: Software Composition Analysis (Analisi della composizione del software)

SBOM: Software Bill of Materials (Distinta base del software)

CNWS: Cloud Networks Security (Sicurezza delle reti cloud)

WAAP: Web Application and API Protection (Applicazione web e protezione API)

Fonte: Frost & Sullivan

Dichiarazione di non responsabilità legale

Frost & Sullivan non è responsabile di eventuali informazioni errate fornite da aziende o utenti. Le informazioni di mercato quantitative si basano principalmente su interviste e sono pertanto soggette a fluttuazioni. I servizi di ricerca di Frost & Sullivan sono pubblicazioni limitate contenenti preziose informazioni sul mercato fornite a un gruppo selezionato di clienti. I clienti riconoscono, al momento dell'ordine o dello scaricamento, che i servizi di ricerca di Frost & Sullivan sono per uso interno e non per la pubblicazione generica o la divulgazione a terzi. Il presente servizio di ricerca non può essere dato, prestato, rivenduto o divulgato, in tutto o in parte, a destinatari diversi dai clienti senza autorizzazione scritta. Non potrà inoltre essere riprodotto, memorizzato in un sistema di recupero o trasmesso in qualsiasi forma o con qualsiasi mezzo (elettronico, meccanico, fotocopia, registrazione o altro), in tutto o in parte, senza l'autorizzazione dell'editore.

Per informazioni sull'autorizzazione, scrivere a: permission@frost.com