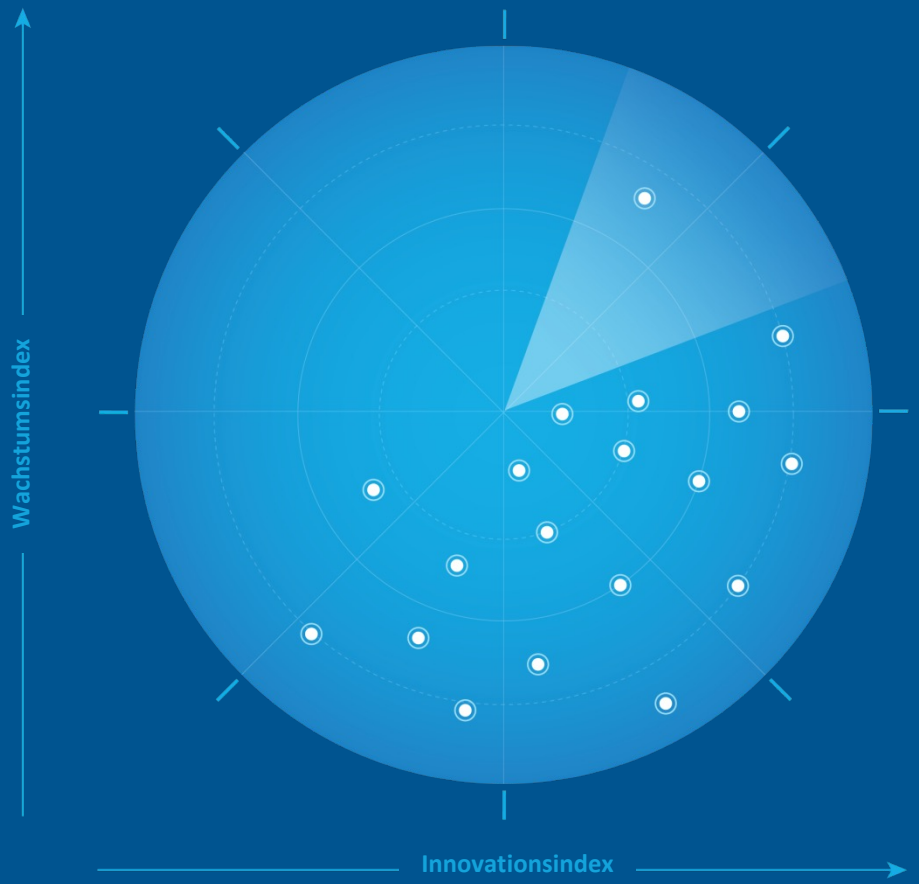
FROST & SULLIVAN

Frost Radar™: Cloudnative Plattformen für Anwendungsschutz (CNAPP) 2022

Ein Benchmarking-System, das Unternehmen zu Spitzenleistungen motiviert – Innovationen, die Pipeline- und Umsatzwachstum fördern



Autor: Anh Tien Vu
Industry Principal, Global Cybersecurity

PD8C-74
November 2022

FROST & SULLIVAN

Kernstrategie und Wachstumsumfeld

Kernstrategie

Cloud-Computing wird mit einer Vielzahl an verfügbaren Cloud-Modellen und -Services allmählich zur Norm in der Wirtschaft. Durch den rasanten Wechsel zur Cloud konnten Unternehmen ihre digitale Transformation vorantreiben und die IT-Infrastruktur sowie ihre Geschäftsabbläufe vereinfachen.

Der Einsatz von Cloud-Computing verändert den Lebenszyklus der Anwendungsentwicklung, die Sicherheitsabläufe sowie die Art und Weise, wie Unternehmen den Aufbau, die Abläufe und die Verwaltung der internen Infrastruktur sowie kundenseitigen Anwendungen mithilfe cloudnativer Technologien (z. B. Container/Kubernetes, serverlose Systeme, IaC (Infrastructure-as-Code)) und anderer CI/CD-Plattformen (Continuous Integration/Continuous Delivery) zur Cloud-Verwaltung, Umsetzung, Entwicklung und Bereitstellung gestalten.

Aufgrund des stärkeren Fokus auf cloudnative Technologien zur Anwendungsentwicklung steigen Unternehmen von einem herkömmlichen monolithischen Anwendungsentwicklungsmodell auf einen Ansatz mit Mikroservices-Architektur und Containern um, der zunehmend quelloffene Abhängigkeiten und Bibliotheken nutzt.

Container/Kubernetes-Technologien und serverlose Datenverarbeitung verändern die Strategien zur Anwendungsentwicklung, da Unternehmen ihre Anwendungen damit flexibel entwerfen, entwickeln, testen und auf den Markt bringen können, wodurch das Benutzererlebnis verbessert wird. Die jährliche Umfrage der Cloud Native Computing Foundation (CNCF) im Jahr 2021 zeigte, dass 96 % der Unternehmen entweder bereits Kubernetes einsetzen oder sich damit beschäftigen. Zudem nutzen derzeit 93 % von ihnen Container in der Produktionsphase oder wollen diese in Zukunft einsetzen. Doch die Nutzung von quelloffenen Software-Anwendungen, Bibliotheken bzw. Abhängigkeiten und Registrierungen führt auch zu mehr Sicherheitsbedrohungen, da diese Anwendungsartefakte für Container-Image-Schwachstellen, Host-Sicherheitslücken, Code-Injektionsangriffe (bei serverlosen Anwendungen) und Compliance-Verstöße anfällig sind.

Quelle: Frost & Sullivan

Kernstrategie (Fortsetzung)

Die zunehmende Komplexität der Hybrid- und Multi-Cloud-Umgebung, die größere Angriffsfläche sowie die Herausforderungen bei der Sicherheitsverwaltung erfordern eine integrierte und cloudnative Plattform, die für Unternehmen Transparenz, Kontrolle und Sicherheit bietet, um moderne Cloud-Computing-Architekturen (z. B. virtuelle Maschinen (VMs), Container, Kubernetes, serverlose Systeme) zu schützen, Sicherheitsmaßnahmen in den Software-Entwicklungszyklus zu integrieren und die Einhaltung von Vorschriften effektiv zu überwachen. Damit ist der herkömmliche Sicherheitsansatz überholt, denn er unterstützt keine Mikrosegmentierung und ist nicht robust genug, um mit den veränderten Anwendungen – insbesondere in Container- und serverlosen Umgebungen – Schritt zu halten.

Aus diesem Grund fordert die CNCF einen Paradigmenwechsel zu einem „Shift-Left and Shield-Right"-Sicherheitsmodell, das cloudnative Anwendungen schützt, indem es Sicherheitsmaßnahmen enger an dynamische Workloads knüpft, die anhand von Attributen und Metadaten (z. B. Label und Tags) identifiziert werden. Bei dem Modell muss Sicherheit bei der Anwendungsentwicklung nicht nur in den späten Phasen, sondern von Anfang an in den gesamten Prozess integriert werden. Zudem sind Sicherheitsmaßnahmen für die Cloud-Umgebung erforderlich, in der die Anwendungen bereitgestellt und ausgeführt werden. Dadurch steigt der Bedarf an einer cloudnativen Plattform für Anwendungsschutz (CNAPP).

CNAPP ermöglicht es Unternehmen, diesen Sicherheitsherausforderungen mit einer integrierten Sicherheitsplattform zu begegnen, statt Einzellösungen wie eine Sicherheitsverwaltung für Cloud-Umgebungen (CSPM), eine Plattform für Cloud-Workload-Schutz (CWPP) oder Schwachstellenverwaltung nutzen zu müssen. Zudem wird die Zusammenarbeit zwischen dem Sicherheits-, dem IT- bzw. Plattform-Team und den Entwicklern verbessert, sodass die Produktivität gesteigert und die Risiken für ihre Cloud-Umgebungen stärker reduziert werden können.

Quelle: Frost & Sullivan

Wachstumsumfeld

Der Umsatz des globalen CNAPP-Markts im Jahr 2021 betrug 1.720,6 Millionen US-Dollar, ein Wachstum von 48,8 % im Vorjahresvergleich. Frost & Sullivan prognostiziert, dass sich dieser Trend mit einer durchschnittlichen jährlichen Wachstumsrate von 25,7 % von 2021 bis 2026 fortsetzt, sodass sich der Umsatz im Jahr 2026 auf 5.406,8 Millionen US-Dollar belaufen wird. Der Grund dafür ist der wachsende Bedarf an einer einheitlichen Cloud-Sicherheitsplattform, die die Sicherheit der Cloud-Infrastruktur stärkt und Anwendungen und Daten über ihren gesamten Lebenszyklus schützt.

Viele Unternehmen nutzen bereits seit einiger Zeit einzelne CNAPP-Komponenten: CSPM für Transparenz und Kontrolle im Rahmen der Cloud-Sicherheit und CWPP für Laufzeitschutz und Compliance. Zudem sind in letzter Zeit die Investitionen in DevOps-Sicherheit gestiegen, da mit dem Shift-Left-Ansatz Sicherheitsmaßnahmen in die frühen Phasen des Software-Entwicklungszyklus integriert werden müssen. Ebenso werden Lösungen für CIEM (Cloud Infrastructure Entitlement Management, Berechtigungsverwaltung für die Cloud-Infrastruktur) und Cloud-Netzwerksicherheit vermehrt von Unternehmen genutzt, die frühzeitig auf cloudnative Lösungen ihrer Cloud-Anbieter umgestiegen sind.

Insgesamt haben Unternehmen weltweit also große Summen in andere Formen von CNAPP investiert. Der größte Teil davon floss in Einzellösungen zur Bewältigung bestimmter Use Cases und Herausforderungen. Das Konzept, all diese Tools im Rahmen einer CNAPP-Lösung zu konsolidieren, ist (ebenso wie die Abkürzung) noch relativ unbekannt, was bei potenziellen Benutzern zu Verwirrung und zu eher zögerlichen Investitionen in die Technologie führen kann. Dennoch werden die Ausgaben für Cloud-Sicherheitstechnologien im Allgemeinen und für CNAPP-Plattformen im Besonderen aufgrund der zunehmenden Implementierung von Cloud-Services und cloudnativen Technologien zur Anwendungsentwicklung sowie der größeren Angriffsfläche in der Cloud-Umgebung steigen.

Quelle: Frost & Sullivan

Wachstumsumfeld (Fortsetzung)

Viele Unternehmen – besonders solche mit einem hohen Reifegrad – sind sich bewusst, dass isolierte Anwendungen, quelloffene Programme und die fehlende Möglichkeit zur schnellen Reaktion auf Bedrohungen für die Infrastruktur und Workloads zu Sicherheitslücken führen und die Komplexität für das Sicherheitsteam erhöhen können. Die Notwendigkeit, Risiken in einer zentralen Übersicht identifizieren, priorisieren und beheben zu können, wird die Nachfrage nach CNAPP-Plattformen steigen lassen.

Unternehmen benötigen eine zentrale Plattform, die besseren Schutz, detaillierte Einblicke und eine effiziente Risikoverwaltung bietet, um Sicherheits- und Compliance-Risiken gemeinsam verwalten zu können. Dies ist mit einer zunehmenden Akzeptanz der Multi-Cloud-Strategie sowie der Notwendigkeit verbunden, Workloads kontinuierlich vor Angriffen zu schützen und die Durchsetzung von Richtlinien für verschiedene Umgebungen zu zentralisieren – ob für die Cloud-Infrastruktur, Container/Kubernetes, IaC oder CI/CD-Pipelines.

Es gibt einen wachsenden Bedarf an besserer Integration von CNAPP in das DevOps-Framework für den Software-Entwicklungszyklus sowie in CI/CD-Pipeline-Plattformen, um den Shift-Left-Ansatz in allen Phasen der Software-Entwicklung (Entwicklung, Tests, Veröffentlichung) umsetzen zu können. Die Integration von CNAPP in DevOps dient dazu, drängende Probleme zu lösen, die bei Scans nach Anwendungsartefakten (Static/Dynamic Application Security Testing [statische/dynamische Sicherheitstests von Applikationen, SAST/DAST], Scans von Anwendungs-Programmierschnittstellen [API], Software Composition Analysis [SCA] und Schwachstellenverwaltung), Cloud-Risiken durch Konfigurationsfehler, Analysen von Laufzeitverhalten und durch Compliance-Vorgaben auftreten. Durch diese Umstellung steigt der Bedarf an cloudnativen Sicherheitslösungen zum Schutz cloudnativer Plattformen, insbesondere für Container/Kubernetes, Hosts, Anwendungsabhängigkeiten, serverlose Anwendungen/Codes, CI/CD-Tools und andere Orchestrierungsplattformen.

Quelle: Frost & Sullivan

Wachstumsumfeld (Fortsetzung)

In Bezug auf den Bedarf werden CSPM, CWPP und DevOps-Sicherheit weiterhin wichtige CNAPP-Funktionen bleiben, doch auch CIEM und Services für Cloud-Netzwerksicherheit werden in den nächsten fünf Jahren an Bedeutung gewinnen. Viele Unternehmen nutzen anscheinend mindestens zwei Komponenten eines Anbieters gleichzeitig, um von besserer Verwaltung und effizienterem Schutz zu profitieren.

Die Konsolidierung von Use Cases für die Cloud-Sicherheit wird sich in den nächsten Jahren fortsetzen. Weitere Anbieter werden sich auf dem CNAPP-Markt etablieren, entweder mit ihren eigenen proprietären oder mit eingekauften Technologien. Unternehmen mit einem umfassenden CWPP-Angebot (z. B. Kaspersky, Fortinet und VMware) werden in den Markt höchstwahrscheinlich mithilfe des Ausbaus oder Ankaufs von Technologien eintreten. Nichtsdestotrotz wird es auf dem Markt voraussichtlich mehr innovative Entwicklung und Wettbewerb durch Startups mit eigenen cloudnativen Sicherheitslösungen geben, die auf CSPM, CWPP und DevOps-Sicherheit ausgerichtet sind.

Von Frost & Sullivan durchgeführte Untersuchungen, die mit dieser unabhängigen Analyse verbunden sind:

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

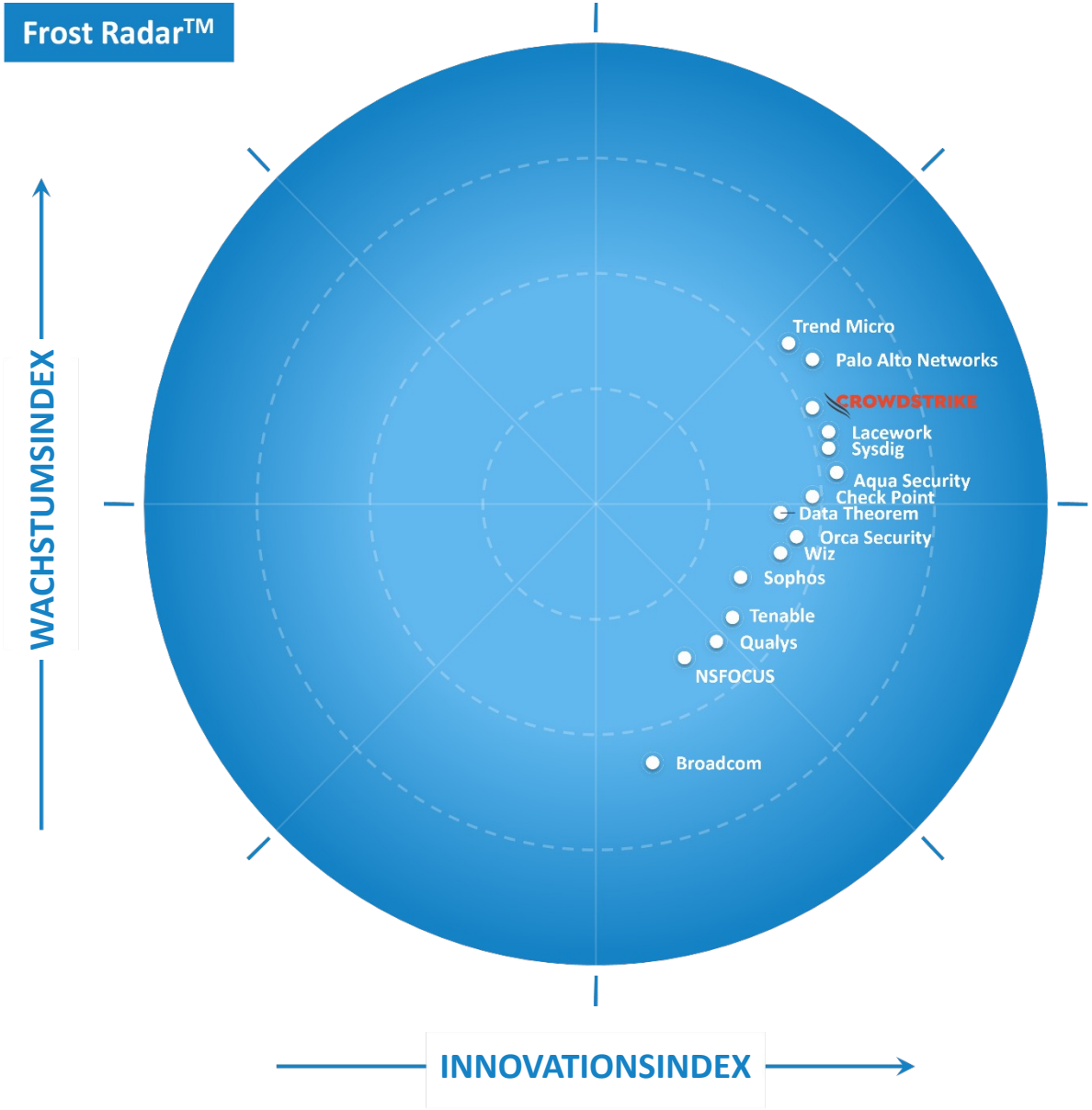
Quelle: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Cloudnative Plattformen für Anwendungsschutz

Frost Radar™: Cloudnative Plattformen für Anwendungsschutz



Quelle: Frost & Sullivan

Frost Radar™

Wettbewerbsumfeld

Der CNAPP-Markt steht noch relativ am Anfang mit Anbietern herkömmlicher Netzwerk- und Endgerätesicherheit, Anbietern für Schwachstellenbewertungen sowie Start-ups, die auf Cloud-Sicherheit spezialisiert sind. Aus einem Feld mit über 20 Branchenteilnehmern weltweit wurden die 15 größten Unternehmen in dieser Frost Radar™-Analyse von Frost & Sullivan unabhängig untersucht. Die im Bericht erwähnten Anbieter erfüllen folgende Kriterien:

- Präsenz in mindestens zwei Regionen (Nordamerika; Europa, Nahost und Afrika [EMEA]; Asien-Pazifik [APAC]; oder Lateinamerika) im Jahr 2021 und in der ersten Jahreshälfte 2022;
- ein jährlicher Umsatz von mindestens 20 Millionen US-Dollar im Jahr 2021 und mindestens 1 % Marktanteil;
- und eine geeignete CNAPP-Plattform bis zum September 2022 (d. h. eine Plattform, die mindestens über CSPM- und CWPP-Funktionen verfügt).

Für diese Frost Radar™-Ausgabe wurden Aqua Security, Broadcom, Check Point Software Technologies, CrowdStrike, Data Theorem, Lacework, NSFOCUS, Orca Security, Palo Alto Networks, Qualys, Sophos, Sysdig, Tenable, Trend Micro und Wiz untersucht. Frost & Sullivan hat festgestellt, dass diese Unternehmen den CNAPP-Markt beherrschen und beeinflussen. Andere Unternehmen sondieren den Markt noch oder haben ihn erst kürzlich betreten.

Mit zunehmender Weiterentwicklung des Marktes werden weitere große Cybersicherheitsunternehmen und Startups im Bereich der Cloud-Sicherheit in den Markt einsteigen. Frost & Sullivan geht davon aus, dass der Wettbewerb auf dem Markt zunehmen wird und dass sich die Landschaft im Hinblick auf Markteintrittsstrategien und technologische Innovationen in den nächsten zwei Jahren deutlich verändern wird.

Quelle: Frost & Sullivan

Frost Radar™

Wettbewerbsumfeld (Fortsetzung)

Ein maßgeblicher Faktor im Entscheidungsprozess von Kunden ist die Fähigkeit eines Anbieters, eine integrierte Plattform bereitzustellen, die Sicherheitsfunktionen konsolidiert und vereinheitlicht. Damit sollen Unternehmen bei der Verwaltung der Sicherheit sowie der Erkennung und Abwehr von Sicherheitsrisiken und Bedrohungen während des gesamten Lebenszyklus der Software-Entwicklung in der cloudnativen Umgebung unterstützt werden. Eine weitere wichtige Rolle spielen professioneller Support, das Preis-Leistungs-Verhältnis sowie ein flexibles und transparentes Preismodell.

Kunden suchen nach umfassenderen Funktionen, die ihnen Transparenz und Sicherheit von der Entwicklung bis zur Produktion für DevOps, DevSecOps und die Cloud-Infrastruktur bieten. Sie wollen also CNAPP-Lösungen, die alle Assets abdecken (Code, Anwendung, Workload und Infrastruktur). Mit diesen Lösungen können sie eine ganzheitliche Sicherheitsstrategie umsetzen und Zero-Trust-Sicherheit in verschiedenen Cloud-Umgebungen gewährleisten.

Immer mehr Unternehmen nutzen Funktionen, die künstliche Intelligenz (KI) bzw. Machine Learning (ML) nutzen, um Risiken in der Cloud-Umgebung zu minimieren. Deshalb werden CNAPP-Lösungen in der Lage sein müssen, Sicherheitsmaßnahmen in die frühen Phasen der Code-Entwicklung zu implementieren sowie KI- und ML-Funktionen zu integrieren. Damit können sie bessere Einblicke in das Verhalten von Workloads und Anwendungen liefern und aufzeigen, wie sich das Verhalten auf die Cloud-Infrastruktur auswirkt. Dies wiederum ermöglicht bessere automatisierte Funktionen zur Bedrohungserkennung und -abwehr.

Der Bedarf an einer umfassenderen Integration des Schutzes von Web-Anwendungen steigt, da diese Schutzmaßnahmen mit denen der zugrunde liegenden Cloud-Workloads gebündelt werden müssen, die diese Web-Anwendungen bereitstellen.

Quelle: Frost & Sullivan

Frost Radar™

Wettbewerbsumfeld (Fortsetzung)

CNAPP-Lösungen können selbst gehostet, im Rahmen einer Partnerschaft von einem Managed Security Services-Anbieter verwaltet oder als SaaS-Modell (Software-as-a-Service) bereitgestellt werden. Die meisten Kunden wählen jedoch ein Cloud-Bereitstellungsmodell, mit dem der Arbeitsaufwand verringert, das Team entlastet und eine höhere Ausfallsicherheit erreicht werden kann. Dies gilt vor allem für kleine und mittlere Unternehmen. Dagegen wird für große Unternehmen und solche in stark regulierten Branchen das selbst gehostete Modell relevant bleiben, da sie Datenschutz- und Compliance-Anforderungen erfüllen müssen.

CrowdStrike wurde für den Wachstumsindex ausgewählt, weil das Unternehmen in den letzten drei Jahren ein starkes und beständiges Wachstum verzeichnete, auch wenn es in Bezug auf den Marktanteil nur an siebter Stelle steht. Frost & Sullivan erkennt den festen Kundenstamm von CrowdStrike, die bessere Markenwahrnehmung sowie den deutlichen Fokus auf Cloud-Sicherheit an. Dadurch wird das Unternehmen sehr wahrscheinlich die Wachstumsdynamik für seine CNAPP-Lösung in den nächsten zwei bis drei Jahren weiter aufrechterhalten können.

Quelle: Frost & Sullivan

FROST & SULLIVAN

Unternehmen in Aktion:

Unternehmen, die vorrangig für Investitionen, Partnerschaften oder Benchmarking in Betracht kommen

CrowdStrike

INNOVATIONEN

- Das CNAPP-Angebot von CrowdStrike besteht aus der agentenbasierten Lösung Falcon Cloud Workload Protection, der agentlosen Lösung Falcon Horizon (CSPM), einer CIEM-Lösung sowie einer Container-Sicherheitslösung, die den Shift-Left-Ansatz im Rahmen der CrowdStrike Falcon-Plattform umsetzt.
- Die Plattform setzt Technologien zur Verhaltensanalyse für die Erkennung malwareloser Bedrohungen und dateiloser Angriffe ein, damit Unternehmen Cloud-Konfigurationsfehler erkennen und verhindern, die Compliance gewährleisten sowie Hosts, virtuelle Maschinen (VMs), Anwendungen und Container/Kubernetes verwalten und schützen können. Dies erfolgt durch eine frühe Identifizierung von Schwachstellen, Bedrohungserkennung und -abwehr, Laufzeitschutz und die Durchsetzung von Compliance-Vorgaben. Diese Funktionen werden zwar über zwei separate Module angeboten, können jedoch über CrowdStrike Falcon bereitgestellt werden, das auf proprietäre Threat Graph-, Asset Graph- und Intel Graph-Datenbanken zurückgreift. Diese Datenbank wird mit Informationen von Endgeräten, Cloud-Workloads, Containern und weiteren Quellen für Telemetriedaten gespeist.

WACHSTUM

- CrowdStrike ist einer der am schnellsten wachsenden Cloud-Sicherheitsanbieter, was vor allem auf seine XDR/EDR- und MDR-Lösungen zurückzuführen ist. Das CNAPP-Geschäft konnte das Unternehmen durch seinen stärkeren Fokus auf den Cloud-Sicherheitsmarkt weltweit ausbauen.
- Den Schätzungen von Frost & Sullivan zufolge stieg der Umsatz von CrowdStrike im CNAPP-Bereich im Jahr 2021 um 71,7 % im Vorjahresvergleich, wodurch es mit einem Marktanteil von 5,0 % zu einem der führenden Anbieter auf dem Markt wurde.
- Obwohl der Großteil des Geschäfts auf Nordamerika entfällt, verzeichnete das Unternehmen im Vorjahresvergleich ein Wachstum von 92,6 % in der EMEA-Region und 82,3 % in der APAC-Region.
- Als einer der am schnellsten wachsenden Anbieter cloudnativer Endgerätesicherheit mit einem zuverlässigen Channel-Partner-Ökosystem kann CrowdStrike seine Cloud-Sicherheitsmodule an große Unternehmen in verschiedenen Branchen weiterverkaufen. Dies wird dazu beitragen, das Wachstum auch künftig aufrechtzuerhalten.

ANALYSE VON FROST

- CrowdStrike hat durch sein CNAPP-Angebot an Bekanntheit gewonnen, da dies in den letzten zwei Jahren weltweit stark gewachsen ist.
- Frost & Sullivan erkennt die Wachstumsdynamik durch eine nachhaltige Pipeline, den durch seine XDR/EDR-Angebote entstandenen festen Kundenstamm und das starke Channel-Partner-Ökosystem. Diese Faktoren werden den geschäftlichen Erfolg im CNAPP-Markt weiter vorantreiben.
- Insbesondere die Fähigkeit, MDR- und Cloud Threat Hunting-Services bereitzustellen, gilt im Vergleich zu anderen Mitbewerbern als Alleinstellungsmerkmal, da dies das Vertrauen der Kunden stärken und das Benutzererlebnis der Lösungen verbessern kann.
- Dennoch sollte CrowdStrike die Anwendungsszenarien für seine CNAPP-Lösung mit anderen Funktionen wie CSPM oder CIEM statt CWPP diversifizieren. Zudem sollte das Unternehmen seine CNAPP-Angebote mit Code-Schwachstellen-Scans erweitern, um seine Plattform umfassender zu gestalten.

Quelle: Frost & Sullivan

FROST & SULLIVAN

Strategische Einblicke

Strategische Einblicke

1

Obwohl der CNAPP-Markt noch am Anfang steht, wird der Wettbewerb durch zahlreiche Anbieter zunehmen, die den Markt in den nächsten zwei bis drei Jahren betreten werden. Dies wird einen enormen Druck auf die bestehenden Anbieter ausüben und sie zwingen, ihre Wettbewerbsvorteile durch technologische Innovationen und Preismodelle aufrechtzuerhalten. Um die Funktionen ihrer Plattform zu verbessern, an Zugkraft zu gewinnen und die Betriebskosten zu senken – und ihren Kunden dennoch besseren Support und ein gutes Benutzererlebnis bieten zu können – werden die Marktteilnehmer angesichts der starken Mitbewerber ihre Anstrengungen in der Forschung und Entwicklung sowie die Maßnahmen für Fusionen und Übernahmen verstärken müssen.

2

Für den Erfolg auf dem entstehenden CNAPP-Markt ist es wichtig, den Markt über die Technologie zu informieren. Die Anbieter müssen eng mit ihren Branchenpartnern zusammenarbeiten, um das Bewusstsein für Cloud-Sicherheit bei globalen Unternehmen und die Bedeutung von CNAPP in deren Cloud-Transformation zu schärfen.
Das Wachstum der Anbieter wird vorwiegend von ihren Channel-Partner-Programmen bestimmt. Deshalb ist es wichtig, dass ein Anbieter die richtigen Channel-Partner hat, die den Markt informieren, für ihre Lösungen werben, mit Kunden in Kontakt treten und diese vor Ort unterstützen können, um ihr Vertrauen und ihre Sympathie zu gewinnen.

3

Die Wahl und der Kauf einer CNAPP-Lösung ist eine Entscheidung, die nicht allein von einem CISO getroffen werden kann. CNAPP erfordert eine umfassendere Zusammenarbeit zwischen den Entwicklungs-, Sicherheits- und IT-Teams, die jeweils ihre eigenen Strategien, Präferenzen und Kennzahlen haben. Zudem muss die Entscheidung mit den CIOs (Chief Information Officers) sowie den leitenden Entwicklern und Managern abgesprochen werden, denn sie alle verfolgen ein gemeinsames Ziel.

Quelle: Frost & Sullivan

FROST & SULLIVAN

Nächste Schritte: Das Frost Radar™ zur Unterstützung wichtiger Verantwortlicher nutzen

Die Bedeutung von Frost Radar™ für Unternehmen

Im Frost Radar™ aufgeführte Unternehmen sind Branchenführer entweder beim Wachstum, in der Innovation oder in beidem. Sie haben einen entscheidenden Anteil an der zukünftigen Entwicklung der Branche.

WACHSTUMSPOTENZIAL

Ihr Unternehmen verfügt über ein erhebliches Wachstumspotenzial in der Zukunft, was es zu einem „Unternehmen in Aktion“ macht.

BEST PRACTICES

Ihr Unternehmen ist sehr gut aufgestellt und hat großen Einfluss auf die Best Practices der Growth Pipeline™ (Wachstumspipeline) in Ihrer Branche.

WETTBEWERBSINTENSITÄT

Ihr Unternehmen sorgt für eine hohe Wettbewerbsintensität im Wachstumsumfeld.

VORTEILE FÜR KUNDEN

Ihr Unternehmen hat gezeigt, dass es sein Wertversprechen deutlich stärken kann.

PARTNERPOTENZIAL

Ihr Unternehmen genießt bei Kunden, Investoren, Partnern der Wertschöpfungskette und dem künftigen Nachwuchs den Ruf, einen bedeutenden Mehrwert zu bieten.

Quelle: Frost & Sullivan

Frost Radar™ unterstützt das Growth Team des CEO

KERNSTRATEGIE

- Wachstum lässt sich immer schwieriger erzielen.
- Die Wettbewerbsintensität ist hoch.
- Es ist mehr Kooperation, Teamarbeit und Fokus gefragt.
- Das Wachstumsumfeld ist komplex.

DAS FROST RADAR™ NUTZEN

- Das Growth Team (Wachstumsteam) hat die nötigen Tools, um eine kooperative Atmosphäre im gesamten Management-Team zu schaffen und somit Best Practices voranzutreiben.
- Das Growth Team verfügt über eine Bewertungsplattform, um das künftige Wachstumspotenzial abzuschätzen.
- Das Growth Team kann den CEO mit einer leistungsstarken Growth Pipeline™ unterstützen.

NÄCHSTE SCHRITTE

- **Growth Pipeline Audit™**
- **Growth Pipeline-as-a-Service™**
- **Growth Pipeline Dialog™ mit Team Frost**

Quelle: Frost & Sullivan

Frost Radar™ unterstützt Investoren

KERNSTRATEGIE

- Die Zahl der Abschlüsse ist gering und der Wettbewerb hoch.
- Due-Diligence wird durch Komplexität in der Branche erschwert.
- Das Portfoliomanagement ist nicht effektiv.

DAS FROST RADAR™ NUTZEN

- Investoren können sich auf künftiges Wachstumspotenzial konzentrieren, indem sie eine Auswahl an Unternehmen in Aktion zusammenstellen, die ein hohes Potenzial für Investitionen haben.
- Investoren können Due-Diligence betreiben, um Geschäfte sorgfältiger und schneller abzuschließen.
- Investoren können die maximal mögliche interne Rendite erzielen und langfristige Erfolge für die Aktionäre sichern.
- Investoren können die Leistung regelmäßig mit Best Practices für optimales Portfoliomanagement vergleichen.

NÄCHSTE SCHRITTE

- **Growth Pipeline Dialog™**
- **Workshop Opportunity Universe**
- **Growth Pipeline Audit™ als obligatorische Due-Diligence**

Quelle: Frost & Sullivan

Frost Radar™ unterstützt Kunden

KERNSTRATEGIE

- Lösungen werden komplexer und haben langfristige Auswirkungen.
- Anbieterlösungen können verwirrend sein.
- Die Votalität unter den Anbietern verstärkt die Unsicherheit.

DAS FROST RADAR™ NUTZEN

- Kunden verfügen über ein analytisches Grundgerüst, mit dem sie potenzielle Anbieter miteinander vergleichen und Partner finden können, die leistungsfähige Langzeitlösungen bereitstellen.
- Kunden können die innovativsten Lösungen bewerten und zudem nachvollziehen, wie die jeweilige Lösung ihre Anforderungen erfüllen würde.
- Kunden erhalten eine langfristige Perspektive für Anbieter-Partnerschaften.

NÄCHSTE SCHRITTE

- **Growth Pipeline Dialog™**
- **Growth Pipeline Diagnostic™**
- **Frost Radar™ Benchmarking-System**

Quelle: Frost & Sullivan

Frost Radar™ unterstützt den Vorstand

KERNSTRATEGIE

- Wachstum lässt sich immer schwerer erzielen, CEOs benötigen Anleitung.
- Die Orientierung im Wachstumsumfeld erfordert komplexe Fertigkeiten.
- Die Wertschöpfungskette verändert sich.

DAS FROST RADAR™ NUTZEN

- Der Vorstand hat ein individuelles Bewertungssystem, um den langfristigen Erfolg des Unternehmens zu kontrollieren.
- Der Vorstand verfügt über eine Diskussionsplattform, bei der die wichtigsten Fragen, Benchmarks und Best Practices zum Schutz der Aktionärsinvestitionen im Mittelpunkt stehen.
- Der Vorstand kann dem CEO mit kompetentem Mentoring, Unterstützung und Governance zur Seite stehen, um das künftige Wachstumspotenzial zu maximieren.

NÄCHSTE SCHRITTE

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

Quelle: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™-Analyse

Frost Radar™: Künftiges Wachstumspotenzial vergleichen

2 große Indizes, 10 Analyseparameter, 1 Plattform

VERTIKALE ACHSE

Der **Growth Index (Wachstumsindex, GI)** ist ein Maß für die Wachstumsleistung und die Erfolgsbilanz eines Unternehmens. Er zeigt die Fähigkeit, eine ideal ausgerichtete Wachstumsstrategie und Vision, eine robuste Wachstumspipeline sowie markt-, wettbewerbs- und endverbraucherorientierte Verkaufs- und Marketingstrategien zu entwickeln und effektiv umzusetzen.

ELEMENTE DES GROWTH INDEX

- **GI1: MARKTANTEIL (IN DEN LETZTEN 3 JAHREN)**
  Dies ist ein Vergleich des Marktanteils eines Unternehmens im Verhältnis zu seinen Mitbewerbern im jeweiligen Markt in den letzten 3 Jahren.
- **GI2: UMSATZWACHSTUM (IN DEN LETZTEN 3 JAHREN)**
  Hier geht es um die Umsatzwachstumsrate eines Unternehmens in den letzten 3 Jahren in dem Markt/der Branche/der Kategorie, die den Kontext für das jeweilige Frost Radar™ darstellt.
- **GI3: WACHSTUMSPIPELINE**
  Dies ein Maß dafür, wie stark die Wachstumspipeline eines Unternehmen ist und wie sehr sie dafür genutzt wird, die vorhandenen Wachstumsmöglichkeiten kontinuierlich zu erfassen, zu analysieren und zu priorisieren.
- **GI4: VISION UND STRATEGIE**
  Dies ist ein Wert dafür, wie gut die Wachstumsstrategie eines Unternehmens auf seine Vision ausgerichtet ist. Stehen die Investitionen, die ein Unternehmen in neue Produkte und Märkte tätigt, im Einklang mit der erklärten Vision?
- **GI5: VERKAUF UND MARKETING**
- Dies ist ein Maß für die Effektivität der Verkaufs- und Marketingbemühungen eines Unternehmens, die die Nachfrage ankurbeln und zur Erfüllung der Wachstumsziele führen sollen.

Frost Radar™: Künftiges Wachstumspotenzial vergleichen

2 große Indizes, 10 Analyseparameter, 1 Plattform

HORIZONTALE ACHSE

Der **Innovation Index (Innovationsindex, II)** ist ein Maß für die Fähigkeit eines Unternehmens, Produkte, Dienstleistungen und Lösungen (mit einem klaren Verständnis für disruptive Megatrends) zu entwickeln. Diese sollen zudem global einsetzbar sein und sich weiterentwickeln sowie erweitern lassen, um mehrere Märkte und sich ändernde Kundenbedürfnisse zu bedienen.

ELEMENTE DES INNOVATION INDEX

- **II1: SKALIERBARKEIT DER INNOVATIONEN**
  Dies ist ein Maß dafür, ob die Innovationen eines Unternehmens im globalen Maßstab auf neuen und etablierten Märkten sowie in angrenzenden und ferneren Branchen skalierbar und einsetzbar sind.
- **II2: FORSCHUNG UND ENTWICKLUNG**
  Dies ist ein Maß für die Effektivität der F&E-Strategie eines Unternehmens, die sich an der Höhe der F&E-Investitionen und der Art und Weise, wie diese in die Innovationspipeline einfließen, ablesen lässt.
- **II3: PRODUKTPORTFOLIO**
  Dies ist ein Maß für das Produktportfolio eines Unternehmen, wobei das Augenmerk darauf liegt, welchen relativen Beitrag neue Produkte zum Jahresumsatz leisten.
- **II4: NUTZEN VON MEGA-TRENDS**
  Dies ist ein Maß dafür, wie proaktiv ein Unternehmen sich entwickelnde, langfristige Chancen und neue Geschäftsmodelle als Grundlage seiner Innovationspipeline nutzt. Eine Erklärung des Begriffs Megatrends finden Sie hier.
- **II5: KUNDENORIENTIERUNG**
  Hier wird die Anwendbarkeit der Produkte/Services/Lösungen eines Unternehmens für aktuelle und potenzielle Kunden bewertet. Zudem wird begutachtet, wie die Innovationsstrategie durch veränderte Kundenbedürfnisse beeinflusst wird.

Anhang

Liste der verwendeten Abkürzungen

CNAPP: Cloud-native Application Protection Platform (cloudnative Plattform für Anwendungsschutz)

DAST: Dynamic Application Security Testing (dynamischer Anwendungssicherheitstest)

IAST: Interactive Application Security Testing (interaktiver Anwendungssicherheitstest)

SAST: Static Application Security Testing (statischer Anwendungssicherheitstest)

CSPM: Cloud Security Posture Management (Sicherheitsverwaltung für Cloud-Umgebungen)

CWPP: Cloud Workload Protection Platform (Plattform für Cloud-Workload-Schutz)

IaC: Infrastructure-as-Code

CIEM: Cloud Infrastructure Entitlement Management (Berechtigungsverwaltung für die Cloud-Infrastruktur)

CI/CD: Continuous Integration/Continuous Delivery

API: Application Program Interface (Anwendungs-Programmierschnittstelle)

SCA: Software Composition Analysis

SBOM: Software Bill of Materials (Software-Stückliste)

CNWS: Cloud Network Security (Cloud-Netzwerksicherheit)

WAAP: Web Application and API Protection (Web-Anwendungs- und API-Schutz)

Quelle: Frost & Sullivan

Haftungsausschluss

Frost & Sullivan übernimmt keine Verantwortung für fehlerhafte Informationen, die von Unternehmen oder Benutzern bereitgestellt werden. Die quantitativen Marktinformationen beruhen in erster Linie auf Befragungen und sind daher Schwankungen unterworfen. Bei den Forschungsleistungen von Frost & Sullivan handelt es sich um spezielle Publikationen mit wertvollen Marktinformationen, die einer ausgewählten Gruppe von Kunden zur Verfügung gestellt werden. Die Kunden nehmen bei der Bestellung oder beim Herunterladen zur Kenntnis, dass die Forschungsleistungen von Frost & Sullivan zur internen Verwendung bestimmt sind und nicht veröffentlicht oder an Dritte weitergegeben werden dürfen. Kein Teil dieser Forschungsleistung darf ohne schriftliche Genehmigung an Dritte weitergegeben, verliehen oder weiterverkauft werden. Zudem darf kein Teil ohne Genehmigung des Herausgebers in irgendeiner Form oder auf irgendeine Art und Weise – elektronisch, mechanisch, als Fotokopie, als Aufnahme oder anders – reproduziert oder in einem Abrufsystem gespeichert werden.

Für Informationen bezüglich der Genehmigung wenden Sie sich bitte an: permission@frost.com