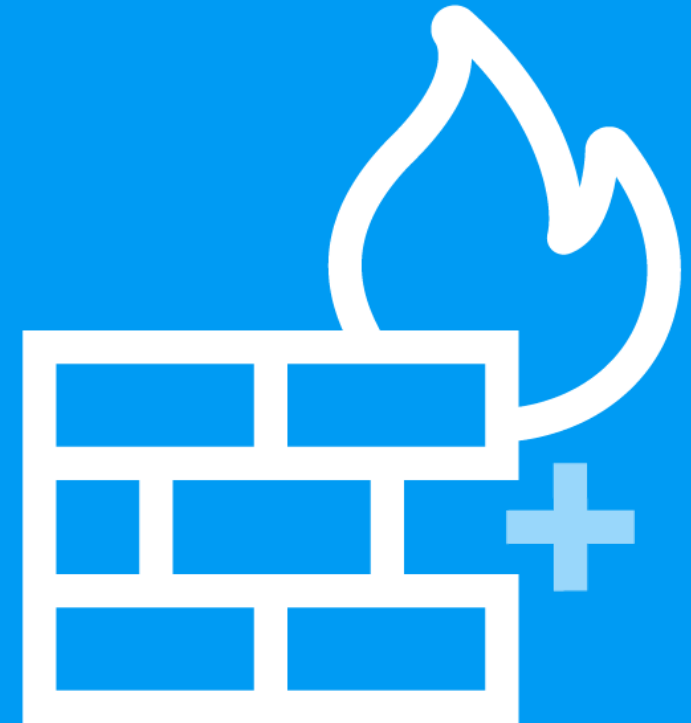


**Next Generation Firewall  
Sales Playbook  
für intern und Partner  
NICHT FÜR ENDKUNDEN**

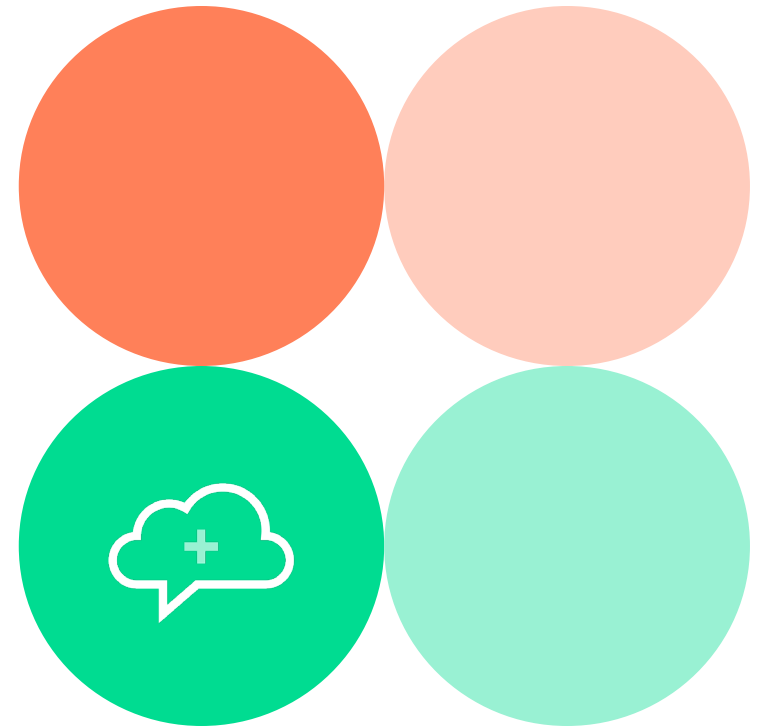


# Was ist ein Sales Playbook?

Dieses Dokument dient der internen Benutzung bei plusserver und Partner-Unternehmen. Es enthält essenzielle Informationen zu Produkten und soll helfen, die Erstgespräche mit Kunden und Interessenten vorzubereiten.

Die Inhalte des Dokuments sind nicht zur Weiterleitung an den Kunden gedacht, dienen vielmehr dem Aufbau eigener Argumentationsketten und sollen u. a. folgende Fragen beantworten:

- + Was kann das Produkt?
- + Für wen ist das Produkt?
- + Wie kann ich die Zielgruppe von den Vorzügen des Produkts überzeugen?  
Welche Argumente und Antworten helfen im Gespräch mit dem Kunden?
- + Wie grenzt sich das Produkt vom Wettbewerb ab?



# Unternehmerische Herausforderungen...

...und Chancen für plusserver

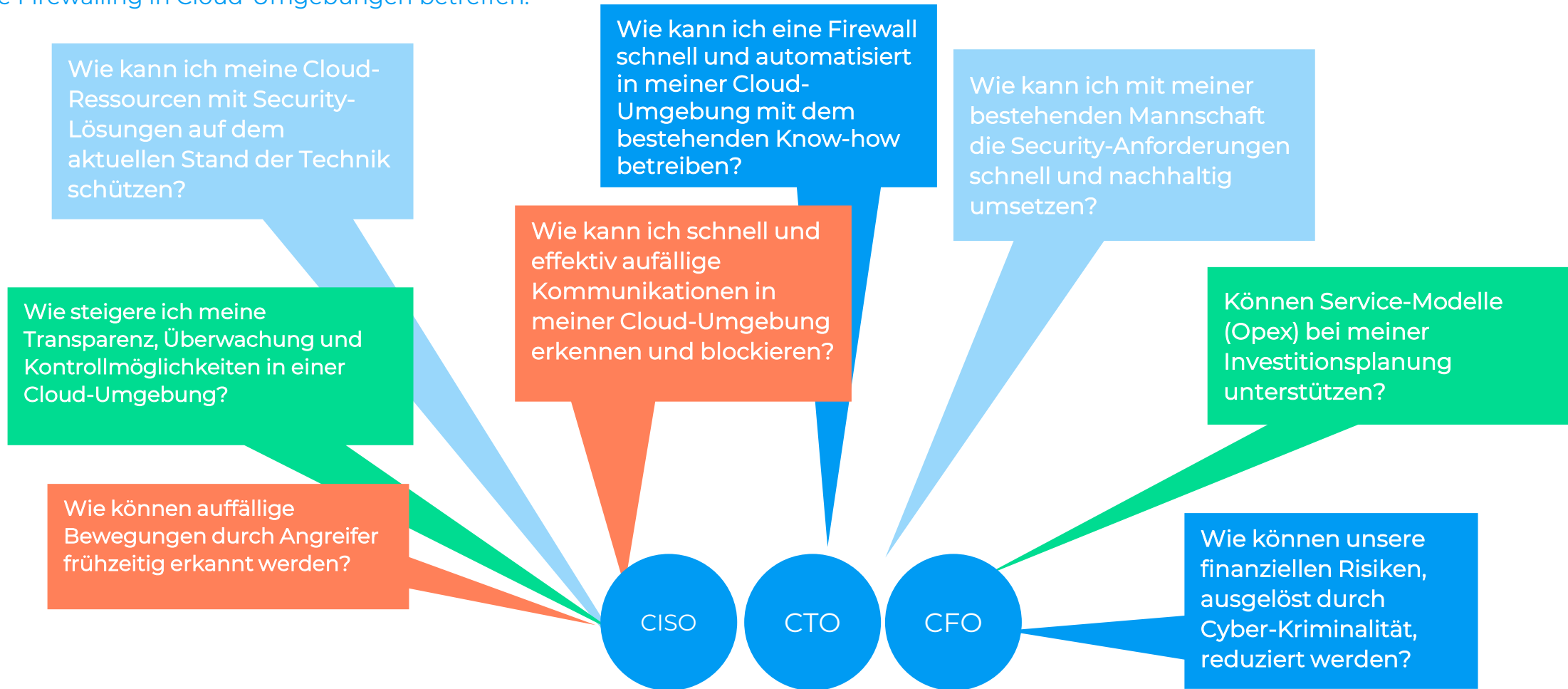
Die Digitalisierung bringt viele Mehrwerte, fordert im Kontext der aktuellen Bedrohungslage aber auch ein generelles Umdenken hinsichtlich einer konsistenten Security-Strategie. Zur Absicherung von Cloud-Infrastrukturen und -Umgebungen gehört auch das Thema Firewalling. Hier besteht die Herausforderung darin, Firewall-Funktionalitäten auf dem aktuellen Stand der Technik in die Cloud zu erweitern, um Ressourcen oder Anwendungen zu schützen. Zu diesen Funktionalitäten zählen die Aufdeckung, Transparenz und Kontrolle über z. B. Schatten-IT oder auch klassische Zugriffe auf Kernapplikationen sowie Ransomware Protection. Die Integration in ein Security Operations Centers (SOC) unterstützt IT-Abteilungen, eine 24x7-Überwachung zu gewährleisten.

Potenzielle Kunden suchen daher nach folgenden Lösungen:

- State-of-the-Art Security in Cloud-Umgebungen
- Schutz vor Angriffen, Malware und Ransomware
- Steigerung der Detektions- und Reaktionsfähigkeit (auch mittels SOC-Integration)
- Erfüllung von Compliance & Regularien in Cloud-Umgebungen

# Fragestellungen,

die Firewalling in Cloud-Umgebungen betreffen:



# Mit plusserver in die Zukunft...

...wie kann mich eine Cloud Firewall oder Dedicated Firewall besser schützen?

Das Produkt **Next Generation Firewalling** ist ein grundlegender Baustein zur Kontrolle, Analyse, Erkennung sowie Verhinderung von Risiken in Cloud-Umgebungen.

- Steigerung der Transparenz und Kontrolle
- Verbindungs- und Zugriffskontrolle
- Schutz vor Ransomware oder Malware
- Intrusion Prevention und Detection
- Applikationssicherheit
- Standardisiertes Regelwerk auf Best-Practise-Ansatz
- Steigerung der Detektions- und Reaktionsfähigkeit mittels SOC-Integration
- Erfüllung von Compliance & Regularien in Multi-Cloud-Umgebungen
- Reduzierte Komplexität durch Servicemodell (Fachkräftemangel)

## Zu schützende Plattformen:



pluscloud  
open



pluscloud  
VMware



Private Cloud



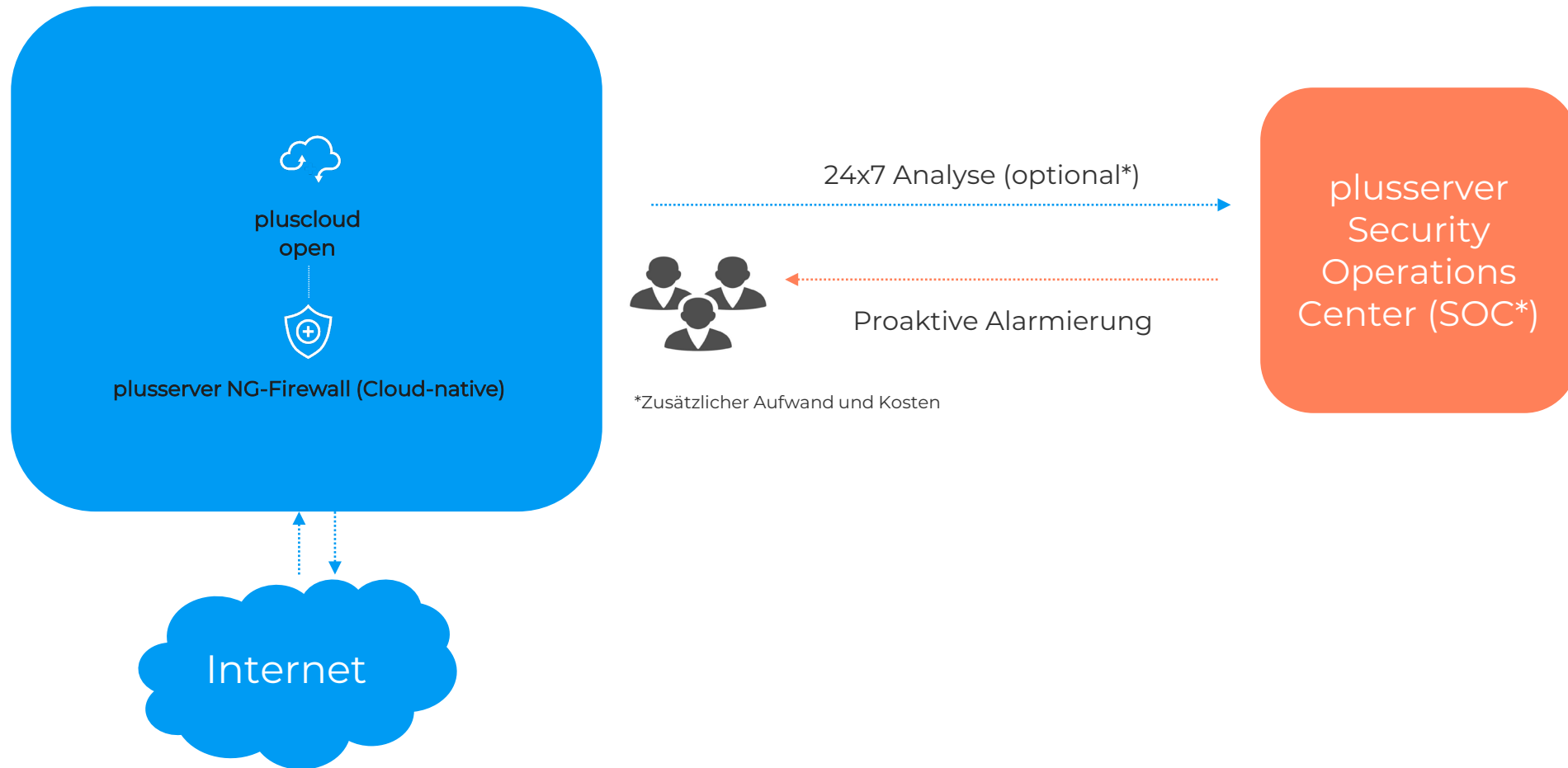
Dedicated Server

# Was gibt es für Möglichkeiten?

## Cloud-native vs. Dedicated

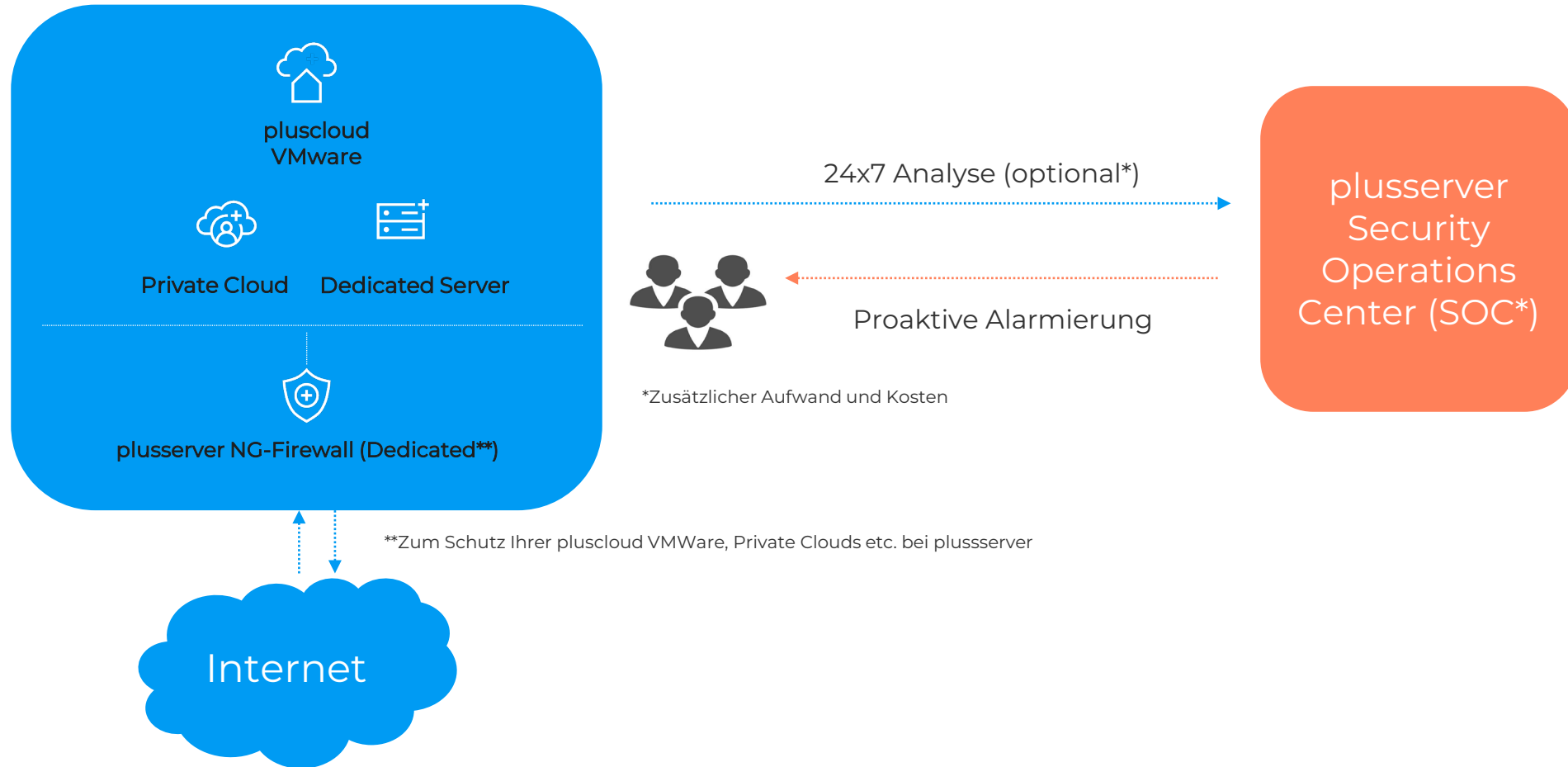
# Next Generation Firewall

Einsatzmöglichkeiten



# Next Generation Firewall

Einsatzmöglichkeiten



\*\*Zum Schutz Ihrer pluscloud VMWare, Private Clouds etc. bei plussserver

# Vorteile & Potentiale

... aus Kundensicht



## IHRE TECHNOLOGISCHEN VORTEILE

- Steigerung der Transparenz und Kontrolle
- Verbindungs- und Zugriffskontrolle
- Schutz vor Ransomware oder Malware
- Intrusion Prevention und Detection
- Applikationssicherheit
- Standardisiertes Regelwerk auf Best-Practise-Ansatz
- Steigerung der Detektions- und Reaktionsfähigkeit mittels SOC-Integration
- Erfüllung von Compliance & Regularien in Multi-Cloud-Umgebungen
- Reduzierte Komplexität durch Servicemodell (Fachkräftemangel)



## UNSERE PRODUKTE

- Next Generation Firewall
  - Cloud-native Firewall (pluscloud open)
  - Dedicated
- SOC-Integration auf Anfrage



## POTENZIALE FÜR IHRE ORGANISATION

- Einsatzmöglichkeit direkt auf der pluscloud open oder als Dedicated Firewall für Ihre Umgebung bei plusserver
- Standardisierte Bereitstellung der Firewall
- Next Generation Firewall Add-on für State-of-the-Art Security Features
- Benachrichtigung über sicherheitsrelevante Ereignisse
- plusserver-SOC-Integration (auf Anfrage)
- Deutschsprachiger Support
- Betrieb in unseren eigenen Rechenzentren in Deutschland, daher DSGVO-konform



## PRICING-MODELL

- Opex-Modell
- Self-Service-Produkt\*
- Individuelle Inbetriebnahme (einmalige Gebühr)

\*Full-Management coming soon!

Next Generation Firewall

# Optionale Inbetriebnahme (Consulting\Self-Services)

Für einen reibungslosen Start des Kunden

Die Inbetriebnahme dauert ca. 5 Personentage und wird mit einem Tagessatz von 1.320 Euro angeboten. Eine SOC-Integration kann nach Rücksprache sowie mit zusätzlichem Aufwand angeboten werden.



\* Erweiterte Professional-Service-Leistungen für Self-Service-Produkte können durch das Security Consulting Team nach Rücksprache mit dem Kunden kostenpflichtig erbracht werden.

# Sprechen Sie uns an

Wir unterstützen Sie gerne bei Ihren Kundenprojekten!

Melden Sie sich einfach bei unserem Channel-Team, um Ihre Projekte und Ideen mit uns zu besprechen. Sie haben Fragen zu unseren Produkten oder wollen Ihr Feedback mit uns teilen? Wir freuen uns über Ihre Nachricht.

Kontaktieren Sie uns jederzeit unter:

Tel.: +49 2203 1045 3500

Mail: [partner.sales@plusserver.com](mailto:partner.sales@plusserver.com)

