plusserver

Endpoint Detection & Response (EDR) as a Service Sales Playbook für intern und Partner

Version 1.2, März 2024

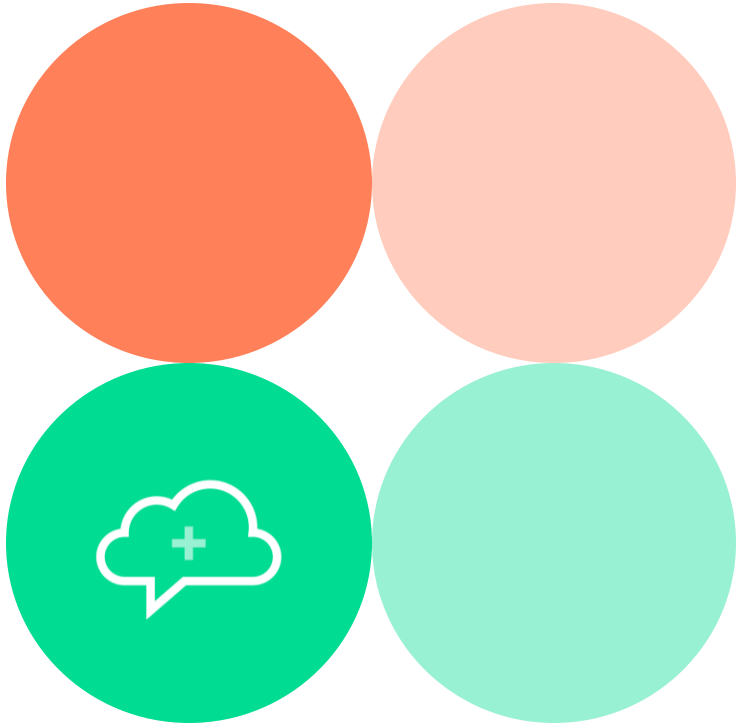
NICHT FÜR ENDKUNDEN

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?



EDR as a Service

… für eine schnelle Vorbereitung eines Kundentermins.

- Moderner Schutz von Daten, Prozessen, Netzwerkverkehr auf Servern und Endpoints
- Verhaltensanalyse und zur Erkennung von zielgerichteten Angriffen
- Malware- und Ransomware-Schutz
- Web- und E-Mail-Schutz auf den Endpoints
- Alarmierung und Reporting
- Managed Service durch plusserver entlastet Ihre IT
- Security by Design, u. a. kontinuierliche Aktualisierung der Plattform
- 24/7-Überwachung durch das plusserver SOC
- Deutschsprachiger 24/7 Support
- DSGVO-konform und CLOUD-Act-neutral

Vorteile & Potenziale der pluscloud open

Unser Service für Ihre Zukunftsfähigkeit

Technologische Vorteile

- Verhaltensanalyse und Erkennung von zielgerichteten Angriffen
- Malware- und Ransomware-Schutz
- Web- und E-Mail-Schutz auf den Endpoints (Integration in den E-Mail-Clients)
- HIPS und NIDS (Host Intrusion Prevention System, Network-based Intrusion Detection System)
- Security-by-Design – beinhaltet die kontinuierliche Aktualisierung
- 24x7 SOC-Integration
- Technologisch immer aktuell durch permanente Weiterentwicklung

Potenziale für Kunden

- Moderner Schutz von Daten, Prozessen, Netzwerkverkehr auf Servern, Cloud und Endpoints
- Full-Managed Service wirkt dem Fachkräftemangel entgegen
- Deutschsprachiger Support
- Alarmierung und Reporting (inkl. Executive Summary)
- Standardisiertes Onboarding und Bereitstellung der Client-Pakete, begleitet durch Consulting
- DSGVO-konform und CLOUD-Act-neutral
- Erfüllung von Compliance-Vorgaben (z. B. NIS2, SIG 2.0)

Pricing-Modell

- Preis pro Endpoint plus SOC-Pauschale (T-Shirt Sizes S, M, L)
- Commitment-Modell mit attraktiven Preisnachlässen
- Opex-Modell
- Individuelles Onboarding (einmalige Gebühr)

Technische Kombinationsmöglichkeiten

... mit anderen plusserver-Produkten

Security & Storage

Security

+ SOC as a Service (obligatorisch)
+ Security Scanner
+ DDoS-Schutz
+ Nex-Gen Firewall

Storage

+ S3 Storage / Object Storage
+ Network Storage
+ Dedicated Storage

Backup & Cloud

Backup

+ Backup as a Service

Cloud

+ pluscloud open
+ pluscloud VMware
+ Dedicated Server
+ AWS, GCP, Azure

Datenbanken & Container

Datenbanken

+ MariaDB as a Service
+ MySQL as a Service
+ PostgreSQL as a Service

Container

+ PSKE, inkl. Workload Protection

Ausgangssituation

… von Unternehmen und öffentlichen Auftraggebern

Security-Verantwortliche stehen vor der Herausforderung, gleichzeitig mit einer steigenden Bedrohungslage (u. a. zunehmende Anzahl von Ransomware-Attacken) sowie einer neuen Arbeitswelt (Homeoffice, mobiles Arbeiten) Schritt zu halten. IT-Sicherheit muss heute jeden einzelnen Endpoint umfassen. Oft sind es die eigenen Mitarbeitenden, die bewusst oder unbewusst Datenverluste oder Ausfälle verursachen.

Potenzielle Kunden suchen daher nach folgenden Lösungen:

+ State-of-the-Art Security am Endpoint
+ Schutz vor Ransomware
+ Steigerung der Transparenz über das Sicherheitslevel im Unternehmen
+ Bessere Detektions- und Reaktionsfähigkeit
+ Schutz hybrider Arbeitsmodellen und neuer Workplace-Strategien (Homeoffice etc.)
+ Abwehr zielgerichteter Attacken

Ausgangssituation

Was ist noch relevant?

Maintenance: Unternehmen möchten sich auf ihr Geschäftsmodell konzentrieren. Der 24/7-Betrieb einer Security-Lösung bleibt oftmals außen vor und wird somit zu einem Risiko für das Unternehmen.

Fehlendes Personal: Der anhaltende Fachkräftemangel wirkt sich hierbei zusätzlich negativ aus, wenn Unternehmen und der öffentliche Sektor sich neben der Entwicklung neuer Geschäftsmodelle und Anwendungen auch um die Sicherheit ihrer Daten kümmern müssen.

Fehlendes Budget: Der Aufbau und die Wartung einer eigenen Security-Infrastruktur sind mit hohen Investitions- und Wartungskosten verbunden.

Auf dem Laufenden bleiben: Unternehmen haben zwar den Wunsch, technologisch auf dem neuesten Stand zu sein. Den Überblick über die neuesten Updates und notwendigen Patches zu behalten, bleibt im Tagesgeschäft jedoch oft auf der Strecke und kann Risiken für den Betrieb bedeuten.

Compliance: Strenge Vorgaben gerade im Behördenbereich verlangen starken Datenschutz, lokale Datenhaltung und Transparenz bei der Auswahl einer geeigneten Lösung.

Die Lösung liefert plusserver

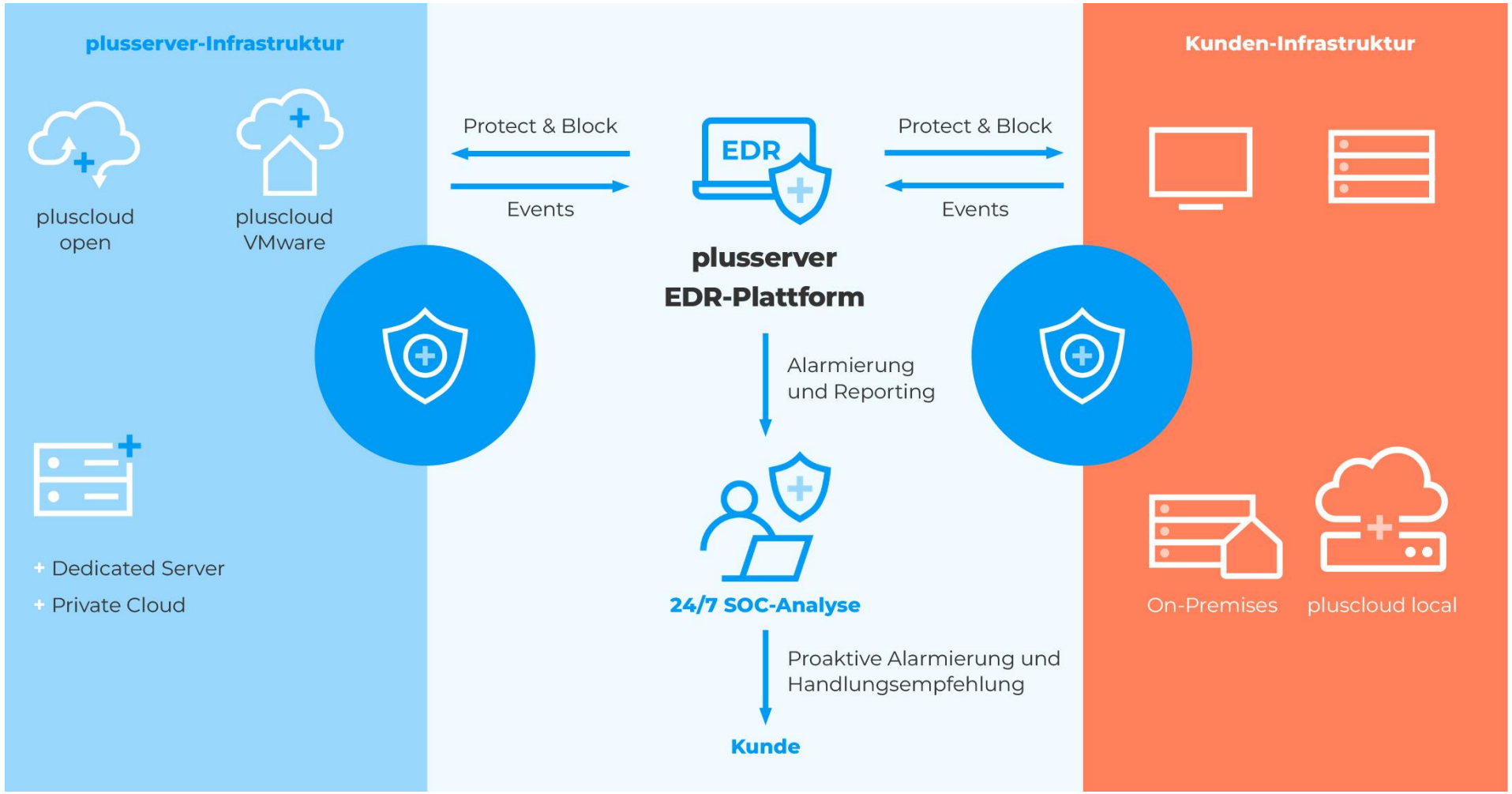
mit EDR as a Service

Endpoint Detection & Response (EDR) as a Service analysiert Ihre Zielsysteme mit modernster Technologie auf bekannte und unbekannte Cyber-Angriffe wie Ransomware oder Malware. Auf Basis dieser Analyse kann die Bedrohungslage auf Endpoints, Servern sowie in der Cloud gezielter eingeschätzt werden. Entsprechende Gegenmaßnahmen können automatisiert eingeleitet werden. Darüber hinaus hilft Ihnen die EDR as a Service-Lösung dabei, Transparenz über Ihr Sicherheitsniveau zu gewinnen.

Ihr PLUS: Um Gefährdungen noch effektiver zu reduzieren, werden die gewonnenen Informationen von Spezialist:innen in unserem Security Operations Center (SOC) analysiert. So können Sie ganz einfach nachhaltige Handlungsempfehlungen für Ihre IT-Umgebung ableiten.

Überwachung sämtlicher Infrastrukturen

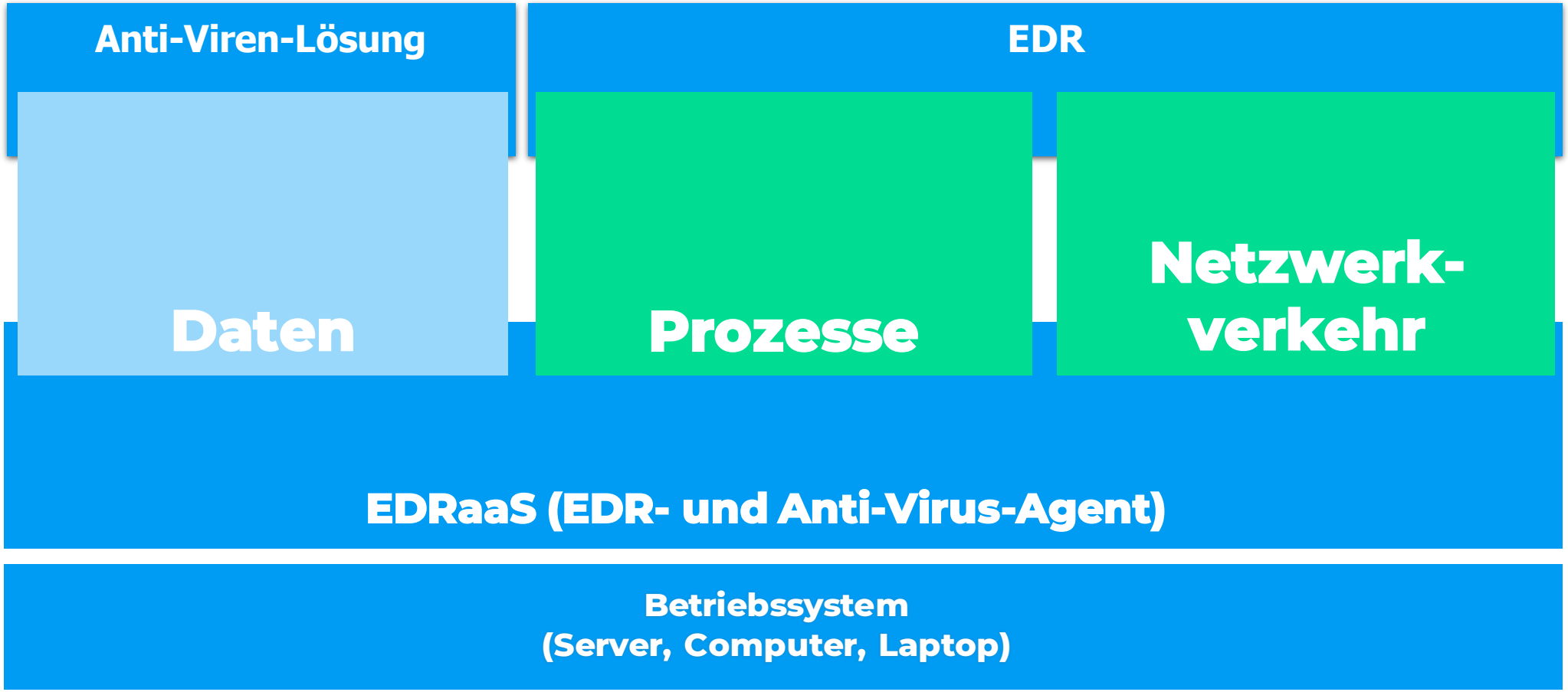
Ob bei plusserver oder beim Kunden



plusserver

EDR vs. Anti-Virus

Warum eine Anti-Viren-Lösung zum Schutz von Endpunkten nicht mehr ausreicht



plusserver

Technologische Basis

Plattformpartner ESET

	Test-Szenarien																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	FPs	Ergebnis
Acronis	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	N	8
Avast	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	N	10
Bitdefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	🛡	N	14
CrowdStrike	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	N	11
ESET	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	N	14
G Data	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	N	12
Kaspersky	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	N	12
Microsoft	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	N	11
VMware	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	N	8

Key		
✓	Bedrohung blockiert, keine C2-Session, System geschützt	1 Punkt
🛡	Kein Alert angezeigt, aber keine C2-Session aufgebaut, System geschützt	1 Punkt
✗	Bedrohung nicht blockiert, C2-Session aufgebaut	0 Punkte
✓	Schutzergebnis ungültig, da auch nicht-schädliche Skripte/Funktionen blockiert wurden	N/A

← **Die ESET-Plattform hat 14 von 15 Angriffssimulationen erfolgreich geblockt.**

plusserver

Standardisiertes Onboarding

Für einen reibungslosen Start des Kunden

Kick-off-Meeting mit dem Kunden
Bestandsaufnahme und Zieldefinition
Vorstellung der Plattform
Erstellung eines kundespezifischen Onboarding-Plans und Konzept (nach Standard)
Vorbereitende Tätigkeiten in der Plattform
Aufbau Regelwerk nach aktuellem Best-Practice-Standard (Detection & Prevention)
Feinanpassung des Regelwerks in Zusammenarbeit mit dem Kunden
Bereitstellung des EDR-Agents für Selfservice oder On-Premise-Installation
Kurzdokumentation und Übergabe an den Kunden sowie plusserver Operations

plusserver

Fragestellungen von Entscheider:innen

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie können auffällige Bewegungen durch Angreifer im Netzwerk erkannt werden?	+ EDRaaS bietet eine Echtzeitüberwachung der Endpoints und erkennt auffälliges Verhalten wie z.B. Veränderung von Daten, Prozessen oder Netzwerkverbindungen.	**Ein Basis-Schutz, unabhängig von den Mitarbeitenden**	✓ Unzureichende Awareness seitens Mitarbeitenden kann Angreifern einen Zugangspunkt in Systeme bieten. Jedoch verfügen nicht alle Mitarbeitenden über ein gleiches Level an Wissen und Awareness rund um Security. EDRaaS liefert einen Basis-Schutz ohne Mehraufwand für die IT – er bietet Sicherheit, ohne auf die aktive Mitarbeit der Mitarbeitenden angewiesen zu sein.
Wie kann ich mit meiner bestehenden Mannschaft die Security-Anforderungen schnell und nachhaltig umsetzen?	+ Mit EDR as as Service erhalten Sie einen Full-Managed Service, sodass Ihr IT-Team nachhaltig entlastet wird. + Zudem werden Sie durch ein individuelles Onboarding unterstützt und können reibungslos mit der Lösung starten.	**Entlastung von IT-Mitarbeitenden**	✓ Ein Security-System aufzusetzen und zu verwalten, braucht nicht nur das entsprechende Fachwissen, sondern ist auch arbeitsintensiv. IT-Abteilungen sind oft bereits mit der Maintenance von Systemen ohne den Security-Layer aus- oder sogar überlastet. ✓ Durch einen Security-Service wird die Verantwortung und operative Arbeit für die Aktualität der Plattform bis hin zur Analyse für Events an den Anbieter abgegeben.

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie kann ich meine Endpoints in einer hybriden Arbeitswelt (Homeoffice) ausreichend schützen?	+ Unser EDR as Service unterstützt Sie dabei, Ihre Digitalisierungsziele zu erreichen, indem Sie Ihre Securitymaßnahmen nachhaltig an Ihr neues Geschäftsmodell anpassen. + Der Dienst greift nicht nur auf Servern oder in der Cloud, sondern auch auf den Endgeräten der Mitarbeitenden, unabhängig vom Einsatzort.	**Unbekannte neue Angriffspunkte durch Vernetzung**	✓ Alles wird vernetzt: Smart Home über New Work bis zu Industrie 4.0 und IoT. Dadurch gibt es viele neue Angriffvektoren, die Unternehmen nicht aktiv auf dem Schirm haben. ✓ Durch EDRaaS können all diese neuen Punkte unkompliziert mit geschützt werden (sofern Betriebssystemunterstützung gegeben).
Können Service-Modelle (OPEX) bei meiner Investitionsplanung unterstützen?	+ Ja, Sie nutzen die volle Flexibilität im On-demand-Modell oder sichern sich noch attraktivere Konditionen im Laufzeitmodell. + Statt in eigene Software und Personal zu investieren, können Sie mit unserem vorteilhaften Service-Modell (Opex) noch einfacher Ihre Investitionen planen.	**Versicherungs-schutz**	✓ Um sich gegen Cyberattacken versichern zu können, muss ein umfangreicher Schutz bestehen. Ein State-of-the-Art-Security-System ist dafür Voraussetzung. ✓ Ein EDR zum Schutz der Endpunkte ist dabei ein hilfreiches Element. Moderne Cybersecurity-Versicherungen verlangen einen entsprechenden Nachweis über solche Security-Systeme mit entsprechenden Komponenten.

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie schützt mich eine EDR-Lösung vor zielgerichteten und klassischen Attacken (z. B. Ransomware oder Malware)?	+ EDRaaS analysiert Ihre Zielsysteme mit State-of-the-Art-Technologie und prüft diese auf bekannte und unbekannte Cyberattacken wie Ransomware oder Malware. + Auf Basis dieser Analyse lässt sich die Bedrohungslage auf Endgeräten, Servern sowie der Cloud gezielter bewerten. Passende Gegenmaßnahmen können automatisiert eingeleitet werden.	**Schutz vor Compliance-Strafen**	✓ Wenn es zu Datenvorfällen gekommen ist, müssen Unternehmen nachweisen, dass sie über einen ausreichend großen Schutz verfügten. ✓ Ist der Nachweis erfolgreich, können sie vorgeschriebenen Strafen entgehen, wie z. B. 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr oder bis zu 20 Mio. Euro bei DSGVO-Verstößen.
Wie kann ich schnell und effektiv auf die neue Bedrohungslage reagieren?	+ Sie erhalten eine detaillierte Alarmierung und Reporting über die gefundenen und blockierten Angriffe auf Ihren Endpoints. + Zudem unterstützen Sie die Analysten aus unserem Security Operations Center (SOC) dabei, die Events zu bewerten und auf Sie zugeschnittenene Gegenmaßnahmen einzuleiten.	**Geld sparen und Attraktivität für neue Mitarbeitende steigern**	✓ Homeoffice wird heute stark nachgefragt und ist ein großer Benefit für Arbeitnehmer:innen. Durch die Absicherung von Endgeräten im Homeoffice, unabhängig von der Security des Heimnetzwerks, können Mitarbeitende auch außerhalb des Büros sicher arbeiten. ✓ Unternehmen erhalten dadurch auch die Freiheit, Standorte zu verkleinern und so Miete zu sparen, wenn Mitarbeitende das Homeoffice präferieren.

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Warum reicht eine klassische Virenlösung nicht mehr aus?	+ Ein EDR-System geht einen Schritt weiter als Anti-Viren-Programme. Falls es einer Bedrohung gelingt, in den Endpunkt einzudringen und ihn zu infizieren, kann sie durch eine tiefgreifende Verhaltensanalyse automatisch erkannt und isoliert werden.	**Security nach Augenmaß – nicht einfach „ganz oder gar nicht“**	✓ Unternehmen werden da abgeholt, wo sie sich auf ihrer Digitalisierungsreise gerade befinden. ✓ Ob schrittweise Legacy-Modernisierung oder Lift&Shift – durch die modulare Bauweise unserer Security- sowie weiterer Angebote können Unternehmen sich ihr System, begleitet durch unsere Beratung, so zusammenstellen, wie sie es brauchen. ✓ Made to fit, mit Raum für individuelle Anpassungen. Nicht ein Standard für alles.
Wie können unsere finanziellen Risiken, ausgelöst durch Cyber-Kriminalität, reduziert werden?	+ Eine erfolgreiche Cyberattacke bringt meist hohe finanzielle Verluste (ø 220.000 €, Quelle. ESET) mit sich. + Durch frühzeitige Erkennung und Isolation reduziert sich die Gefahr, Opfer einer zielgerichteten Attacke zu werden bzw. kann das Ausmaß der Schäden reduziert 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