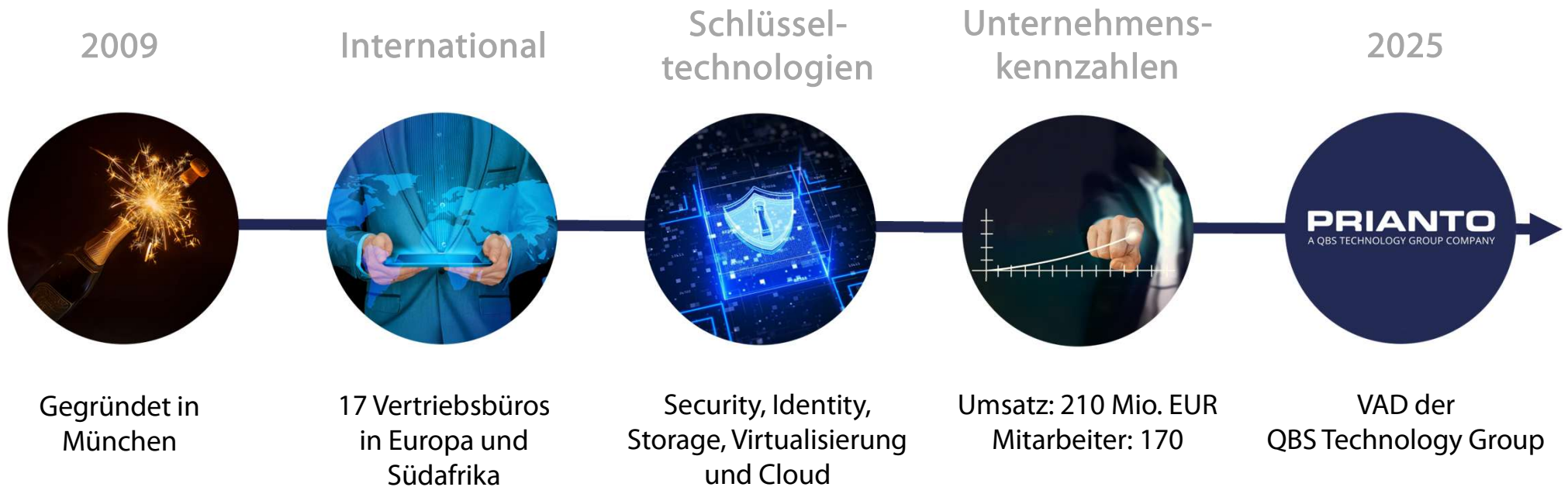


**Mit Sicherheit
Erfolgreich!**



Ihr spezialisierter Value Added Distributor für Enterprise Software



„Es ist unsere Mission, ein zuverlässiger Partner für Reseller, Systemintegratoren und Managed Service Provider zu sein und innovative Softwarelösungen zu verbreiten, welche die digitale Infrastruktur und Arbeitsumgebungen von Unternehmen effizienter gestalten.“



Top Trends Cybersecurity 2025 (Markt und Unternehmen)

- **KI als Cyberwaffe.** Künstliche Intelligenz wird immer mehr von Angreifern (Deep Fake, Ransomware,..) und Verteidigern genutzt.
- **Zero-Trust Architektur.** Unternehmen setzen verstärkt auf diese Strategie, um sich vor Gefahren bei der Nutzung von Cloud-Diensten und mobilen Geräten zu schützen.
- **Resilienz auch für Lieferketten.** Unternehmen achten immer mehr auf die Sicherheit ihrer Software Lieferketten.
- **Cybersecurity-as-a-Service.** Cloud basierte Sicherheitslösungen gewinnen an Bedeutung.
- **Regulierung und Resilienz.** Die Gesetzgeber werden aktivere Maßnahmen zur Cybersicherheit und zum Datenschutz einführen.
- **Proaktive Security Maßnahmen.** Unternehmen können dadurch die Auswirkungen von Cyberangriffen begrenzen.
- **Neue Authentifizierungsmethoden** erhöhen die Sicherheit in Unternehmen.

(Quellen: u.a. Gartner, Forrester Research, KuppingerCole Analysts)

Top Trends Cybersecurity 2025 (Reseller und Systemhäuser)

- **Verunsicherung der Kunden.** Wirtschaftliche Unsicherheiten und Verzögerungen bei Investitionen können die Nachfrage weiter beeinflussen.
- **Ressourcenknappheit.** Der Mangel an qualifizierten Cybersecurity Experten bleibt bestehen.
- **Wachstumspotenzial.** Neue Vorschriften, die zunehmende Digitalisierung und ein größeres Bewusstsein für Cyberbedrohungen steigern das Interesse an Cybersecurity und Identity Security.
- **Die Komplexität der Bedrohungen** erfordert den Einsatz von innovativen und neuen Sicherheitslösungen.
- **Partnerschaften.** Durch die Zusammenarbeit mit anderen, spezialisierten Unternehmen können Angebote und Dienstleistungen erweitert werden.
- **Kundenbindung.** MSP-fähige Lösungen erhöhen die Kundenbindung und garantieren regelmäßige Umsätze.

Managed Service Provider Modelle 2025

Operator

- Betreiben die Lösung selbst (Cloud, on prem) und bieten sowohl dedizierte als auch shared Services an
- Übernehmen volle Betriebsverantwortung

Cloud Service Provider

- Hosten und betreiben SaaS Lösungen in ihrer eigenen Cloud und stellen diese den Kunden zur Verfügung
- Übernehmen volle Betriebsverantwortung

Value-Added SaaS Reseller

- Weiterverkauf von SaaS-Produkten die durch zusätzliche Dienste wie Schulungen oder Support erweitert werden
- Übernehmen keine Betriebsverantwortung

Multi-Cloud Service Provider

- Stellen SaaS Lösungen über mehreren Cloud-Plattformen hinweg bereit und verwalten diese
- Übernehmen keine Betriebsverantwortung

Bitdefender

Quest
Partner Circle

LOGPOINT

Scalefusion

wallix

ONE IDENTITY™

enclave

KELAR

TEHRIS
FACE THE UNPREDICTABLE

nevis®

SailPoint

GUARDIAN 360°

FORENOVA+

riskrecon
by

Belden
macmon

opentext™

freshworks

Prianto Hersteller für Managed Service Provider

	Bitdefender	enclave	ForeNova	Freshworks	Guardian 360	KELA	Logpoint	macmon	Nevis	One Identity	OpenText	Quest	RiskRecon	SailPoint	Scalefusion	Suse	Tehtris	WALLIX
Operator	✓	✓					✓	✓	✓	(✓)		(✓)		✓		✓	✓	✓
Cloud Service Provider	✓	✓					✓	✓	✓					✓		✓	✓	✓
Value-Added SaaS Reseller	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-Cloud Service Provider	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

(✓ = wird unterstützt, (✓) = wird teilweise unterstützt)

Marktführer bei Endpunktsicherheit

- Schützt seit 2001 mehrere Millionen Systeme und Umgebungen von Privatanwendern und Unternehmen. Wo Schutz auf höchstem Niveau sich mit dem Pioniergeist wachsender Unternehmen vereint. Bewährte Prävention, Sicherheit, Erkennung und Abhilfemaßnahmen mit Unterstützung branchenführender Experten.
- Bitdefender GravityZone Business Security
- Bitdefender GravityZone Business Security Premium
- Bitdefender GravityZone Business Security Enterprise
- Bitdefender MDR + MDR PLUS
- Bitdefender GravityZone CSPM+

Bitdefender[®]
BUILT FOR RESILIENCE

Warum Bitdefender?

Europäischer Anbieter



On Premise und
Cloud verfügbar



On-Premise Cloud

Modulares
MSP-Programm



20 Jahre Erfahrung in
Cybersicherheit



Ihr Zugang zur Cloud-Sicherheit der nächsten Generation

- Enclave bietet vertrauliches Cloud-Computing an, das höchste Sicherheit und Datenschutz gewährleistet. Sie ermöglichen es Unternehmen, Anwendungen in sicheren Umgebungen zu entwickeln, zu starten und zu skalieren, wobei die Daten selbst vor dem Cloud-Anbieter geschützt sind. Ihre Lösungen umfassen vertrauliche virtuelle Maschinen, Kubernetes-Cluster und Datenbanken, die Daten selbst während der Nutzung verschlüsseln.
- Schützt Daten in allen drei Zuständen – im Ruhezustand, während der Übertragung und während der Verarbeitung.
- Selbst der Cloud-Anbieter oder Systemadministrator hat keinen Zugriff auf die Inhalte



Warum enclave?

Europäischer Anbieter
- DE -



MSP-Programm mit 100%
Channel-only



Funktioniert mit allen
Cloud Anbietern



20 Jahre Erfahrung in
Netzwerksicherheit



Effektive Abwehr gegen Cyber-Bedrohungen

- Mit fortschrittlicher Erkennung und Reaktion bietet ForeNova KMUs einen erschwinglichen 24/7-Schutz durch ein Team von Cybersecurity-Experten und eigener Technologie. So ermöglicht ForeNova die fortschrittlichste Echtzeit-Erkennung und -Reaktion für Endpoints und Netzwerke und bietet einen umfassenden Schutz über den gesamten Angriffslebenszyklus.
- Schnellere Erkennung und Reaktion auf der Grundlage von kundenspezifisch modellierten GPTs
- Erweiterte Funktionen wie Mikrosegmentierung, Hot Patching und Ransomware-Honeypot
- Inspektion von verschlüsseltem Datenverkehr

FORENOVA

Warum ForeNova?

Europäischer Anbieter



Für KMU geeignet



ISO 27001 zertifiziert



Branchen- führende SLAs



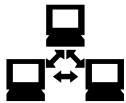
ITSM auf Enterprise-Niveau – für jedes Unternehmen

- Freshservice ist eine cloudbasierte IT-Service-Management-Plattform, die Unternehmen dabei unterstützt, ihre IT-Abläufe zu optimieren. Sie bietet umfassende Funktionen, um die Effizienz zu steigern und die Servicequalität zu verbessern. Durch die Integration von KI und maschinellem Lernen ermöglicht Freshservice eine intelligente und kontextbasierte Servicebereitstellung
- Incident Management
- Automatisierung von Workflows
- IT-Asset-Management
- Integration in Cloud- und On-Prem-Anwendungen



Warum Freshworks?

Nutzung von KI



Für KMU geeignet



Von Analysten ausgezeichnet



Amortisationszeit von <3 Monaten



Der dauerhafte Penetrationstest für schlanke IT-Budgets

- **Guardian360** ist die perfekte Lösung für Unternehmen in regulierten Branchen, die Security und Compliance Frameworks einhalten müssen, ohne kostspielige SIEM- oder SOC-Lösungen implementieren zu müssen. Die Lösung scannt Netzwerke auf Schwachstellen oder Sicherheitslücken und meldet diese im Dashboard, so dass Unternehmen permanent die Kontrolle über ihr Netz haben.
- Tägliche Scans aller offenen Netzwerk Ports und Webanwendungen
- Tägliche Scans von aktuellsten Threat Intelligence-Quellen
- Guardian360 Audits für alle wichtigen Normen (z.B. GDPR, NIS2, TISAX, ISO 27001)



Warum Guardian360?

Europäischer Anbieter
- NL -



MSP-Programm mit 100%
Channel-only



POC und Support
Unterstützung



Automatisierte Audits
(z. B. NIS2)



„Secure the Unseen – No More Blind Spots“

- KELA bietet umfassende Lösungen zur Identifizierung und Analyse von Bedrohungen, die speziell auf die Kunden zugeschnitten sind. KELA nutzt automatisierte Prozesse und Expertenwissen, um relevante Bedrohungen aus dem Darknet zu erkennen und Maßnahmen zur Verbesserung der Cybersicherheit zu unterstützen.
- Threat Intelligence
- Third Party Risk Management
- Identity Theft Protection
- Brand Protection



Warum KELA?

Über 10 Jahre Erfahrung



Modularer Aufbau der Plattform



Attraktives Partner-Programm



In der Praxis geprüft

FAVORABLE REVIEW

5.0 ★★★★★ September 16, 2024

Experience Unparalleled Monitoring on Deep Web and Dark Web

User-friendly experience while using their platform in monitoring deep web and dark web. Alert notifications are easy to configure with more context and precision.

Unified simplicity – convert data into actionable intelligence

- **Logpoint** bietet Unternehmen eine zentrale Cyber Defense Platform, um Bedrohungen zu erkennen, zu analysieren und darauf effektiv zu reagieren. Logpoint ist mehr als nur eine führende SIEM-Lösung. Mit Logpoint lösen Unternehmen Datensilos auf und reduzieren dadurch Komplexität und erhöhen die Benutzerfreundlichkeit.
- **Next-Gen SIEM** mit optionalen Modulen für:
 - Automation (SOAR)
 - Case Management
 - Behavior Analytics (UEBA)



Warum Logpoint?

Europäischer Anbieter



EAL 3 zertifiziert



Flexible Bereitstellung



Unerreichte Automatisierung



Intelligent einfach für Netzwerke und Cloud

- macmon hat sich auf Zero-Trust-Network-Access-Lösungen spezialisiert und unterstützt so Unternehmen dabei, ihre Netzwerksicherheit zu verbessern und Compliance-Vorgaben einzuhalten. Sie bieten herstellerunabhängige Lösungen zur Verbesserung der Transparenz und der Zugriffskontrolle in Netzwerke und für Cloud-Ressourcen.
- **macmon NAC** – Bietet Netzwerkzugangskontrolle, um unbefugten Zugriff zu verhindern und vollständige Transparenz über alle Geräte im Netzwerk zu gewährleisten
- **macmon SDP** – Schützt die Kommunikation mit Unternehmensressourcen in der Cloud und in lokalen Netzwerken durch granulare Zugriffskontrolle

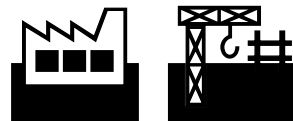


Warum macmon?

Europäischer Anbieter
- DE -



Für IT, OT und Cloud



BSI zertifiziert



20 Jahre Erfahrung in
Netzwerksicherheit



„Making Security an Experience“

- Nevis ist ein Pionier in der digitalen Sicherheit und macht sich weltweit für den Einsatz passwortloser, benutzerfreundlicher Zugangslösungen stark.
- Als Schweizer Marktführer im Bereich Customer Identity and Access Management (CIAM) stützt Nevis Organisationen aus dem Finanz-, Versicherungs- und iGaming-Sektor mit einem Höchstmaß an Datenschutz und nahtlosen Authentifizierungsverfahren aus.
- Identity Suite – Kundenidentitäts- und Zugriffsmanagement für Unternehmen
- Authentication Cloud – schnell, einfach, benutzerfreundlich und sicher

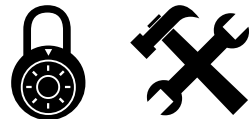


Warum Nevis?

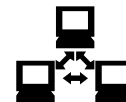
80 % Online
Banking In CH



Höchste Flexibilität
und Sicherheit



Nutzung von KI



Attraktives
Partnerprogramm



Machen Sie IAM zum Herzstück einer Sicherheitsstrategie

- One Identity bietet moderne Identitätslösungen, die angesichts unzähliger menschlicher und maschineller Identitäten, der raschen Migration in die Cloud und der zunehmenden Remote-Arbeit unerlässlich sind. One Identity ermöglicht den Schutz und die Vereinheitlichung der vier Kernelemente der Identitätssicherheit.
- Identity Governance and Administration
- Access Management
- Privileged Access Management
- Active Directory Management



Warum One Identity?

80 % der Fortune
100-Kunden



Über 500 Mio. verwaltete
Identitäten



Von Analysten
ausgezeichnet



On Premise und
Cloud verfügbar



On-Premise Cloud

„Cybersecurity made simple“

- OpenText Security-Lösungen unterstützen Unternehmen jeder Größe dabei, ihre wertvollsten und vertraulichsten Informationen zu schützen. Das Portfolio sich ergänzender Sicherheitslösungen bietet Security Experten einen 360-Grad-Einblick in Endgeräte und Netzwerkverkehr. Dadurch können sie anomales und schädliches Verhalten proaktiv identifizieren, bewerten und untersuchen.
- Application Security
- Identity & Access Management
- Data Privacy & Protection
- Threat Detection & Response

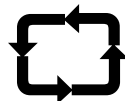
opentext™

Warum OpenText?

95 % der Top 100
Unternehmen



Umfassendes
Portfolio



Von Analysten
ausgezeichnet



On Premise und
Cloud verfügbar



On-Premise Cloud

Der Zukunft einen Schritt voraus

- Seit 1987 bietet Quest Softwarelösungen für die hochdynamische Welt der Unternehmens-IT. Die Lösungen schützen und unterstützen Benutzer und Daten, optimieren den IT-Betrieb und stärken die Cybersicherheit in Unternehmen auch in hybriden Umgebungen von Grund auf.
- **Cybersicherheit und Notfallwiederherstellung**
(z.B. Security Guardian, Recovery Manager, KACE)
- **Migration und Modernisierung**
(z.B. On Demand Migration, Migrator Pro for AD, SharePlex)
- **Data Management & Intelligence**
(z.B. erwin, Foglight, Toad for Oracle)

Quest®

Warum Quest?

97 % der Fortune
500 Unternehmen



Produkte plattform-
übergreifend



On-Premise Cloud

Erstklassiger Support



Bewährte Erfahrung



Achieve better risk outcomes for enterprises and supply chain

RiskRecon bietet als cloudbasierte Plattform präzise Risikobewertungen von Drittanbietern in Echtzeit, wodurch Unternehmen fundierte Entscheidungen treffen und ihre IT-Infrastruktur stärken können. RiskRecon wurde 2015 gegründet und ist mittlerweile ein Tochterunternehmen von Mastercard.

Die wichtigsten Use Cases der Plattform sind:

- Automatisierte Risikobewertung von Lieferanten
- Proaktive Überwachung und Visualisierung der Supply Chain
- Due Dilligence (Cybersicherheitslage) bei Fusionen und Übernahmen
- Situational Awareness



Warum RiskRecon?

Markführer seit 2015



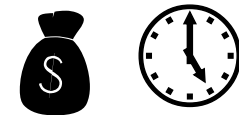
> 97 % Genauigkeit



Einfachste Integration



Messbarer Business Value



Der Kern der Unternehmenssicherheit ist Identity Security

- Das moderne Unternehmen sichern – heute und in Zukunft. Das SailPoint Ziel besteht darin, jede Art von Identität zu erkennen, zu sichern und zu verwalten. Als Teil des Thoma Bravo-Portfolios hat SailPoint die Möglichkeit, Innovationen im Unternehmen voranzubringen, um noch schneller zur Identitätsplattform der Wahl für moderne Unternehmen zu avancieren.
- Mit **Identity Security Cloud** verwalten und sichern Unternehmen den Echtzeit-Zugriff auf wichtige Daten und Apps jeder Unternehmensidentität in einer einheitlichen Weise:
 - Standard = Zentralisieren und vereinheitlichen der Identitätssicherheit
 - Business = Automatisieren und optimieren mit KI in Echtzeit
 - Plus = Reduzierung von Risiken und Vereinfachung von Prozessen mit fortschrittlicher Intelligenz



Warum SailPoint?

50 % der Fortune
50 Unternehmen



Weniger Risiko:
66 % bei Zugriffsrechten



Geringere Kosten:
60 % bei Onboarding



Von Analysten
ausgezeichnet



Einheitliche Verwaltung. Vertrauenswürdige Sicherheit.

- Scalefusion ist eine umfassende **Unified Endpoint Management (UEM)**-Lösung, die Unternehmen dabei unterstützt, ihre Geräte, Anwendungen und Daten zentral zu verwalten und abzusichern. Die Plattform vereint drei leistungsstarke Produkte - Endpunktmanagement, Zero-Trust-Access und Endpunktsicherheit - in einer einzigen, einheitlichen Plattform, die von einem Agenten für alle Betriebssysteme und Geräte betrieben wird.
- **Scalefusion UEM** – zur Verwaltung verschiedenster Geräte (Windows, macOS, iOS, Android, Linux, ChromeOS) inklusive Funktionen wie App-Verteilung, Kiosk-Modus, Remote-Zugriff und Compliance-Überwachung.
- **OnelDp** – für sicheren Zero-Trust-Zugriff mit Multi-Faktor-Authentifizierung und rollenbasierter Zugriffskontrolle.
- **Veltar** – für moderne Endpoint-Sicherheit mit Fokus auf Schutz, Effizienz und Datenintegrität.



Warum Scalefusion?

Betriebssystem-
übergreifend



Ausgezeichnetes
Partnerprogramm



ISO 27001 zertifiziert und
SOC-2 Typ-2-konform



Über 10 Jahre Erfahrung



Zuverlässig, anpassungsfähig, hochverfügbar, sicher und konform

- SUSE ist ein weltweit führender Anbieter von innovativen, zuverlässigen und sicheren Open-Source-Lösungen für Unternehmen. Mehr als 60 % der Fortune-500-Unternehmen vertrauen auf SUSE, um ihre unternehmenskritischen Workloads zu betreiben und überall Innovationen zu ermöglichen - vom Rechenzentrum über die Cloud bis hin zum Edge und darüber hinaus.
- **SUSE Linux Enterprise Server (SLES):** Ein sicheres und anpassbares Betriebssystem für die Bereitstellung und Verwaltung von Workloads in verschiedenen Umgebungen.
- **Cloud- und Edge-Lösungen:** Unterstützung für Public und hybride Clouds sowie schnelle und zuverlässige Datenverarbeitung an der Edge.
- **SAP-Lösungen:** Optimierte Plattformen für den Betrieb von SAP-Anwendungen



Warum Suse?

Über 10 Jahre Erfahrung



Für IT, OT, Cloud, Edge...



60 % der Fortune
500-Kunden



Ausgezeichnetes
Partnerprogramm



Automatische Neutralisierung von Cyberangriffen

- Die **TEHTRIS XDR AI-Plattform** wurde entwickelt, um die wichtigsten Anforderungen für Detection und Response zu erfüllen. Durch den Einsatz eines Netzwerks aus leistungsstarken Sensoren, einschließlich der EDR- Komponenten, verbessert sie den Schutz, die Erkennung und die Reaktionsmöglichkeiten bei Netzwerkangriffen erheblich.
- TEHTRIS XDR AI Plattform: Umfassende Suite mit integrierten Komponenten für SOAR, EDR, SIEM, MTD und NTA.
- TEHTRIS CYBERIA eine kontextbezogene, KI basierte Erkennung und Vorhersage von Sicherheitsbedrohungen auf höchstem Niveau.



Warum Tehtris

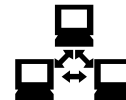
Europäischer Anbieter
- FR -



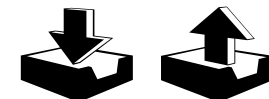
All-in One Cybersecurity



Nutzung von KI



Steigerung SOC-
Produktivität



Cybersecurity Simplified“ – Digitale Assets effektiv geschützt

- Als Marktführer im Bereich **Privileged Access Management** und mit einer Strategie, die auf Innovation und Agilität basiert, hat es sich WALLIX als europäischer Anbieter zur Aufgabe gemacht, die Cybersicherheit für seine Kunden in IT- und OT Umgebungen zu vereinfachen.
- WALLIX PAM und WALLIX Remote Access
- WALLIX IaaS und WALLIX Enterprise Vault
- WALLIX IAG
- WALLIX ONE (Security as a Service)



Warum WALLIX?

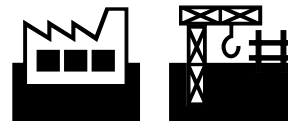
Europäischer Anbieter
- FR -



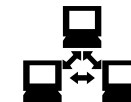
Von Analysten
ausgezeichnet



Für IT und OT



MSP fähig



Grow together – Warum Prianto?



Grow together - Prianto Services für Reseller



Exklusive Management Events zum Aufbau von Netzwerk und Partnerschaften



Regelmässige Schulungen und Workshops zu Produkten und Fachthemen



Umfassender Sales und Technical Support in allen Phasen des Verkaufsprozesses



Durchführung von Co-Marketingmaßnahmen mit Herstellern zur Leadgenerierung



Unterstützung bei Finanzierungs- und Kreditlimit Management



Fokussierung auf Security und Identity Themen



Cross-Selling Potenziale durch ein attraktives Portfolio aus bekannten Marktführern und kleineren Innovationsführern

Grow together - weitere Prianto Services für MSP (MSSP)



Unterstützung beim Auf- und Ausbau des MSP-Geschäftes



Dedizierter Ansprechpartner für alle MSP-Themen



Flexible Abrechnungsmodelle (inklusive monatlicher oder verbrauchsorientierter Abrechnung)



Flexible Nutzung und Einsatz der Prianto MSP-Lösungen



Spezielle Events und Trainings für MSPs zum Aufbau von Know-how, Networking und Partnerschaften

Grow together - Prianto Events: Networking, Partnerschaften, Wissensaustausch



Partner Summit 2025
15. und 16. Mai

Quest
ONE IDENTITY™

freshworks Bitdefender **PRIANTO**
A QBS TECHNOLOGY GROUP COMPANY

Grow together – Warum Prianto?

„Wir arbeiten gerne mit Prianto als Distributor, weil wir sie als zuverlässig, schnell und flexibel kennengelernt haben. Auch die persönliche Kommunikation passt – die Chemie stimmt“

- Thomas W Barth , Country Manager DACH , Intragen -

„Schon früher haben wir gerne mit Prianto zusammengearbeitet und freuen uns sehr darüber, dass wir wieder im One Identity Bereich mit ihnen tätig werden dürfen. Unsere Partnerschaft zeichnet sich durch hohes Vertrauen und kontinuierlichen Erfolg aus.“

- Christian Rückert, Sales Manager Identity- & Accessmanagement, IPG GmbH Deutschland -

Kontakt

Prianto GmbH

Barthstraße 18
80399 München

Tel: +49 89 416148210

Fax:+49 89 416148211

kontakt@prianto.com

Christian Vogel

Business Development Manager MSP

Tel.: +49 1579 2628271

christian.vogel@prianto.com



Follow us on:



A photograph of two business professionals shaking hands outdoors. The person on the left is wearing a light blue shirt, a striped tie, and dark trousers. The person on the right is wearing a tan blazer. The background is a blurred outdoor setting with a bright sun creating a lens flare effect. The text is overlaid in the center of the image.

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf eine erfolgreiche Zusammenarbeit.