TD SYNNEX

SECURITY bei TD SYNNEX Austria 2025

HPE Tour – Mai 2025

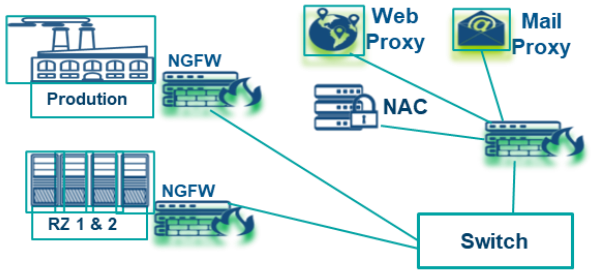
Johannes Föger

Cyber Security Lösungen

TD SYNNEX

MOBILE SECURITY

BORDER SECURITY



SOC SOFTWARE

Security Service Edge SSE/SASE

ACCESS MANAGEMENT

IAM – Identity Access Management
PAM – Privileged Access Management
MFA – Multi-Faktor Authentisierung

CLOUD SECURITY & CLOUD-BASED SECURITY

TD SYNNEX

Unser Security Portfolio

Schutz der Daten & Informationen…

Multi-Faktor-Authentifizierung

IDEE

Endgeräte Sicherheit

SONICWALL
paloalto NETWORKS
BlackBerry
Lookout

E-Mail-Sicherheit

SONICWALL
Barracuda

Zugriffsmanagement

ONE IDENTITY
Authorized Distributor
WALLIX CYBERSECURITY SIMPLIFIED
SpyCloud

Firewall

paloalto NETWORKS
Barracuda
SONICWALL

Cloud-to-Cloud Backup

Barracuda

Management

SIEM, SOAR, XDR

paloalto NETWORKS
BlackBerry
Secureworks
exabeam
Barracuda

SSE & SASE

SONICWALL
Barracuda
paloalto NETWORKS
Lookout

…lokal gespeichert, im Rechenzentrum, in der Cloud oder aus dem Internet.

Strategie

TD SYNNEX

paloalto NETWORKS

Palo Alto Networks Security mit Plattform-Ansatz

Strata	Next-Gen-Firewalls
SASE	Secure Access Service Edge
Prisma Cloud	Cloud-Native Security
Cortex	Sicherheitsautomatisierung
Unit 42	Bedrohungsanalyse & Beratung

Palo Alto Networks Übersicht

Strata-Firewalls	SASE	Prisma	Cortex	Unit 42
PA – Hardware **VM – Software** **CN – Software** **Panorama Firewall Management** **Cloud Delivered Security Services CDSS**	**Prisma Access** FWaaS Secure Webgateway ZTNA ADEM **Prisma SD-WAN** Next-Generation SD-WAN Solution	**Prisma Cloud** Cloud Workload Protection Cloud Security Posture Management Cloud Infrastructure Entitlement Management Cloud Network Security	**Cortex XDR** Endpoint Detection and Response **Cortex XSOAR** Extended Security Orchestration, Autom. and Response **Xpanse** Attack Surface Management	**Proaktiver Assesment Service** **Threat Intelligence** **Digital Forensics and Incident Response**

Partner werden bei PAN

Verkaufen und/oder integrieren

Bereitstellung von Dienstleistungen (Beratung, Schulung und Risikohaftung)

Erstellen, Verkaufen und Verwalten von PAN basierten Sicherheitsdiensten

Anbieten von cloudbasierten Plattformen, Infrastruktur, Anwendungen und/oder Speicherdienste

Palo Alto Networks

Endkunden

Finanzdienstleister: Sie nutzen Palo Alto Networks für ihre Netzwerksicherheit. Sie schätzen die umfassenden Sicherheitslösungen, die sowohl Netzwerk- als auch Cloud-Sicherheit bieten

Gesundheitswesen: Sie setzen auf Palo Alto Networks, um ihre medizinischen IoT-Geräte zu sichern. Dies hilft ihnen, eine effektive und sichere Patientenversorgung zu gewährleisten

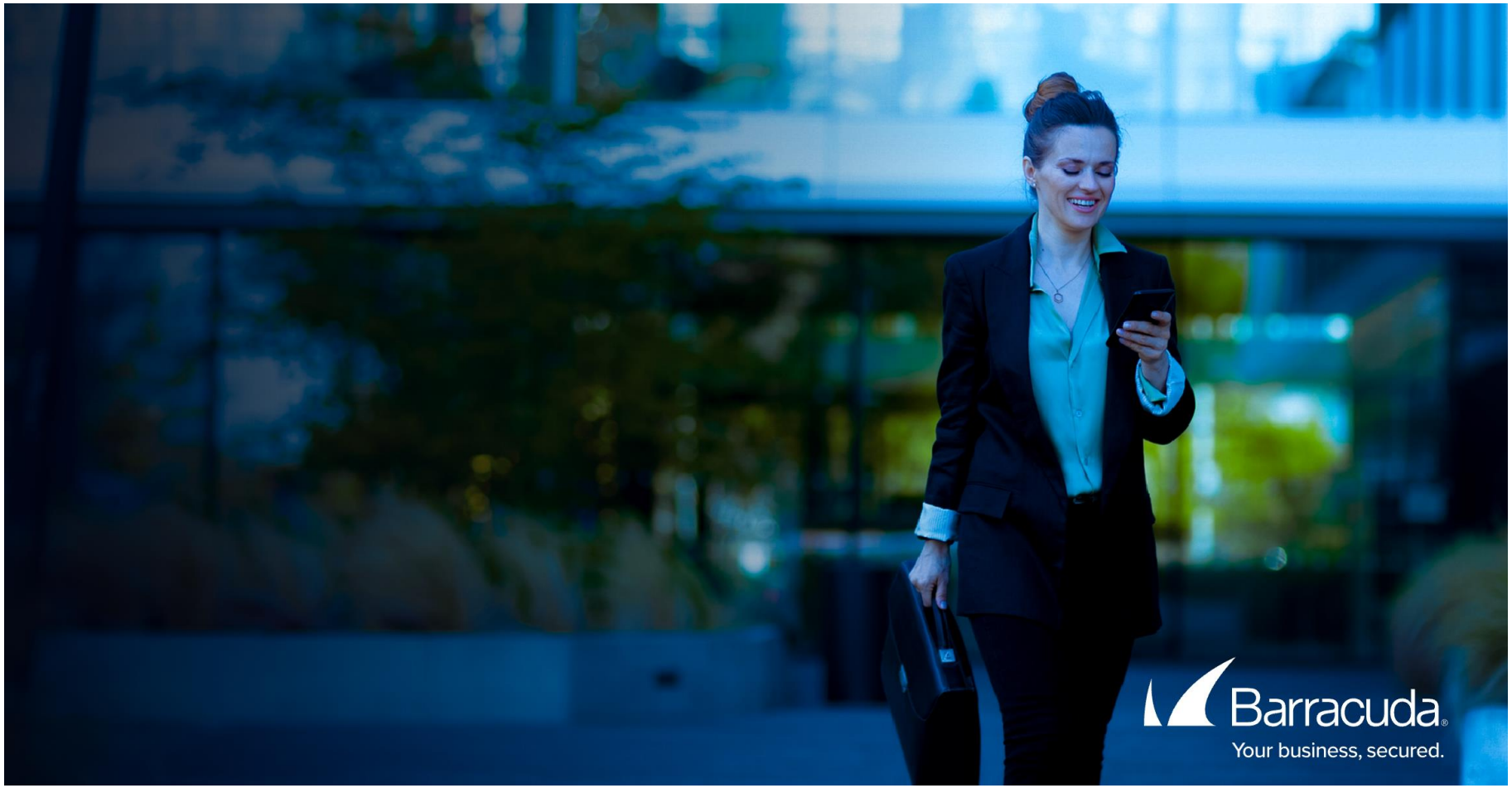
Fertigungsunternehmen: Sie verwenden Palo Alto Networks für sichere und intelligente Fertigungsstätten. Diese Unternehmen profitieren von einer verbesserten Sicherheitsstrategie, die das Wachstum unterstützt

Immobilienentwicklung: Dienstleister für Hauseigentümer modernisieren ihre Sicherheitskonzepte mit Palo Alto Networks. Dies ermöglicht ihnen eine konsolidierte Strategie für Netzwerk-, Cloud- und Endpunktsicherheit

Telekommunikation: Telekommunikationsanbieter nutzen Palo Alto Networks, um Cyberangriffe abzuwehren und den Betrieb aufrechtzuerhalten. Dies ist besonders wichtig für die Aufrechterhaltung der Konnektivität und Sicherheit in dieser Branche, SOC Center

Barracuda

Firewalls, EMail-Prodection, XDR-Lösung, Datensicherung, Anwender-Security



Barracuda Networks

gegründet 2003

1.800 Mitarbeiter weltweit

über 5000 Reseller weltweit

180 Mitarbeiter in AT

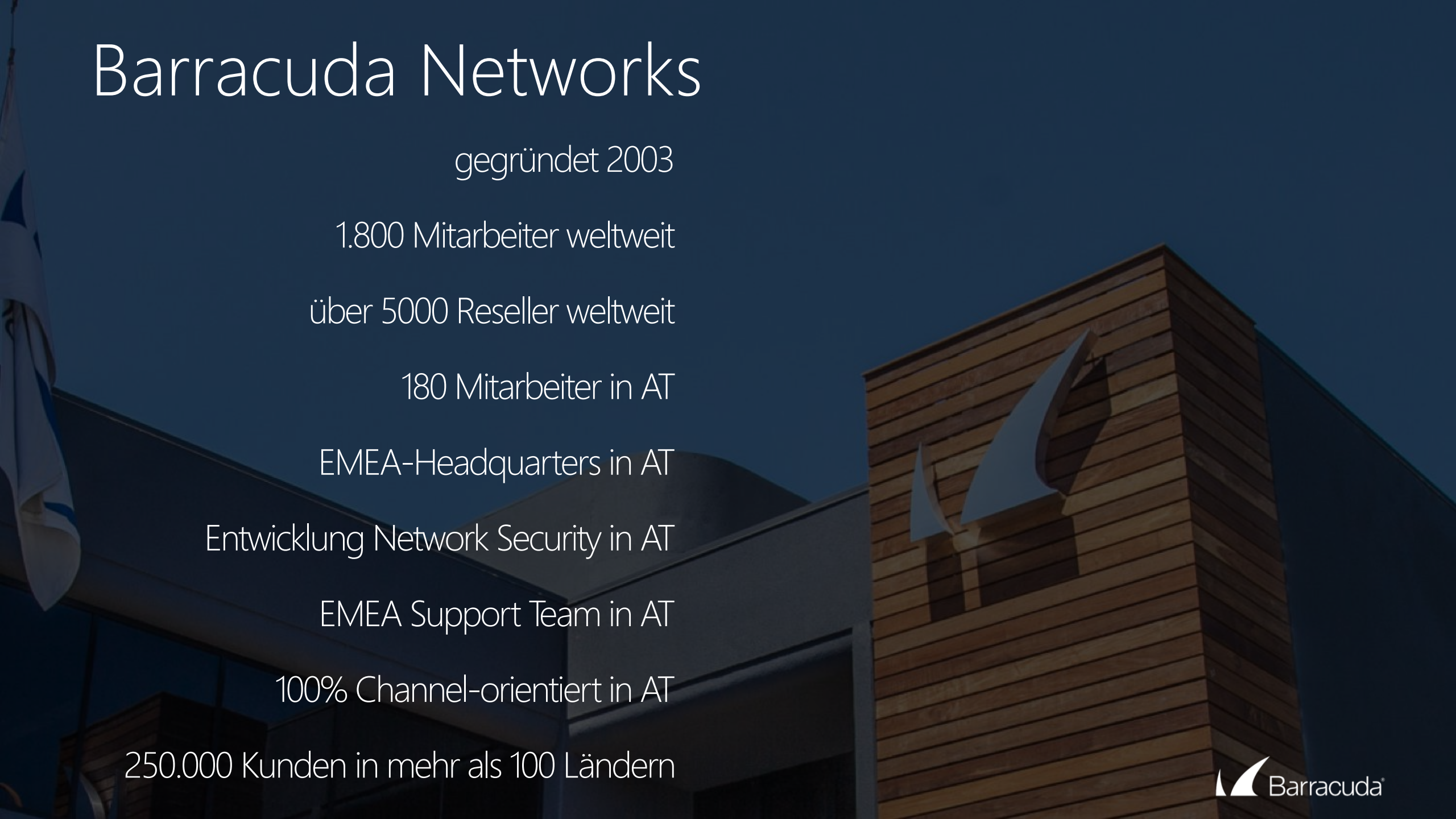
EMEA-Headquarters in AT

Entwicklung Network Security in AT

EMEA Support Team in AT

100% Channel-orientiert in AT

250.000 Kunden in mehr als 100 Ländern



Barracuda

Barracuda Portfolio

Managed Services / XDR

Deployment Choices / Flexible Consumption

Email Protection

- Spam, Malware, Threats
- Phishing & Impersonation
- Account Takeover
- Incident Response
- Security Awareness

Data Protection

- Backup
- Archiving
- Data Classification

Network Protection

- Secure Access Service Edge
- Zero Trust Security
- Secure SD-WAN
- Network Firewalls
- IoT/OT Security

Application Protection

- OWASP Top 10
- Bot Protection
- DDoS Protection
- Client-side Protection
- API Security

Product Platforms

Threat Intelligence Platform

Award-Winning Support

SC awards EUROPE

Best Customer Service

Start als Barracuda Partner

- Einstieg als Authorized Partner
- Zugang zu Deal-Regs (Projektschutz)
- Core und MSP Partnerschaft möglich
- Zugang zu kostenlosen NFR Lizenzen
- technische Unterstützung in der PreSales Phase
- Marketing-Unterstützung
- Zugang zum Support-Team mit jeweiliger Seriennr.
- Professional Service mit Barracuda AT-Mitarbeitern möglich
- Zugang zum Campus-Portal https://campus.barracuda.com/

Zielgruppe

- Unternehmen aller Branchen mit 2 bis 2000 Mitarbeitern

Barracuda Sales Team Austria

Christian Baar
Regional Sales Director Austria
0664 883 74 071
cbaar@barracuda.com

Markus Futschek
Channel Sales Manager
0664 883 74 106
mfutschek@barracuda.com

Markus Sethaler
Field Account Manager AT-Ost
0664 883 74 085
msethaler@barracuda.com

Fabio Lair
Field Account Manager AT-West
0664 883 74 108
flair@barracuda.com

Jan Kirch
Inside Sales – AT-Ost
0512 219 330 1070
jkirch@barracuda.com

Ugur Gündüz
Inside Sales – AT-West
0512 219 330 1076
uguenduez@barracuda.com

Marketing

Benjamin Paliwoda
Field Marketing Manager
0664 883 740 93
bpaliwoda@barracuda.com

Michael Holzer
Sales Engineer
0699 150 49 176
mholzer@barracuda.com

Philipp Ortner
Sales Engineer
0664 883 74 105
portner@barracuda.com

Renewals

Martina Proctor / Anna Stochla
Renewals Representatives
+44 0118 338 4614
dachrenewals@barracuda.com

Barracuda

Endkunden

Fertigungsunternehmen: Barracuda schützt Industrieanlagen und IT-Steuerungssysteme vor Ransomware und fortschrittlichen Cyberbedrohungen

Einzelhandel: Einzelhändler nutzen Barracuda, um ihre Kunden und Unternehmensmarken vor hochentwickelten Cyber-Bedrohungen zu schützen

Bildungseinrichtungen: Schulen und Universitäten setzen Barracuda ein, um Studierende und Fakultäten vor Ransomware und anderen Cyberangriffen zu schützen und die Compliance mit Vorschriften für sicheres Lernen zu gewährleisten

Gesundheitswesen: Barracuda hilft Gesundheitsorganisationen, Patientendaten zu schützen und Störungen zu vermeiden, die die Patientenversorgung beeinträchtigen könnten

Finanzdienstleister: Finanzdienstleister sind ein Hauptziel für Cyberangriffe und nutzen Barracuda, um ihre Daten und Systeme zu sichern

Landes- und Kommunalverwaltung: Behörden auf Landes- und Gemeindeebene verwenden Barracuda, um ihre Websites und Daten zu schützen

Sonicwall

Next Gen Firewalls, Mobile Access, EMail-Security, Network-Security Manager

Company overview

Over 30+ years relentless focus on cybersecurity

Global Footprint

500,000+ customers in 215 countries and territories

Industry Veteran Team

Trusted **+30-year** veteran of the cybersecurity industry

End-to-End Portfolio

Comprehensive cybersecurity **product and service platform**

Global Threat Intelligence Network

Hundreds of terabytes, artifact threat data

100% Channel

17,000+ global channel partners

Cybersecurity Innovation

More than **300 innovative patents** granted, including RTDMI™

SONICWALL®

NEVER ALONE. RELENTLESS SECURITY.

Product Portfolio

High end: NSsp series

Designed for large distributed enterprises, data centers and MSSPs, offering high-speed protection, high port density and up to 100 Gbps firewall inspection throughput.

Mid range: NSa series

Industry-validated security effectiveness and performance for mid-sized networks, branch offices and distributed enterprises.

Entry level: TZ series

Integrated threat prevention and SD-WAN platform for home, small/medium organizations and SD-Branch deployments.

Virtual: NSv series

Virtual firewalls with flexible licensing models to shield all critical components of your public and private cloud infrastructure.

SonicWall Switch

Delivers intelligent switching for next-Generation secure connectivity of SMB and SD-Branch deployments.

Email Security

A multi-layered solution that protects Against advanced email threats; delivered.In appliance, VM and cloud SaaS form Factors.

SonicWave Series

Security and performance build for the next wave of wireless devices, managed through the cloud or firewall with Wi-Fi 6 capable.

SMA Series

Simple, policy enforced secure access to Network and cloud resources.

Cloud Secure Edge

SSE solution that securely connects users to applications, resources and infrastructure while protecting them from internet threats.

Capture Client

Unified client platform that delivers multiple Endpoint Detection & Response (EDR) capabilities.

Network Security Manager

Deploy and manage all your firewalls, connected switches and access points, from one easy-to-use dashboard.

Wireless Network manager

Leverage the ultimate flexibility and reliability of the cloud with SonicWall Wireless Network Manager.

Analytics

High-performance management and reporting engine for your network.

Managed Security Services – MDR, CDR & NDR

Reduce risks and costs with a SonicWall SecureFirst Managed Security Service Provider. Ensure your network is secure and compliant with flexible managed services, including health and performance monitoring, configuration management, and security alerts.

SONICWALL®

DEFENSE ACROSS THE ATTACK SURFACE

SonicSentry Managed XDR

Alert Management · Threat Hunting · Threat Mitigation
Log Retention · Reporting

MDR for Endpoint

Protection and response for endpoints

CROWDSTRIKE

Capture Client

SentinelOne

Microsoft Defender

SOPHOS

MDR for Network

Protection and response at the perimeter

Any network device from any maker

MDR for Cloud

Protection and response for cloud apps and email

Cloud Email Security

Microsoft 365

Google Workspace

Cloud Threat Analytics

slack

Dropbox

salesforce

PROGRAM BENEFITS AT A GLANCE

	VELOCITY TRACK		MASTERY TRACK	
	BRONZE	SILVER	GOLD	PLATINUM
	PROTECT		POWERED	POWERED +
Product Discounts	$	$ $	$ $ $	$ $ $ $
Deal Registration	✓	✓	✓	✓
NFR Access	✓	✓	✓	✓
On-Demand Sales and Technical Training	✓	✓	✓	✓
Co-Branded Marketing Material	✓	✓	✓	✓
Use of SonicWall Logo	✓	✓	✓	✓
Listed on Partner Locator	✓	✓	✓	✓
MDF/SDF Access		✓	✓	✓
Quarterly Rebates		✓	✓	✓
Featured on Partner Locator			✓	✓
Enhanced Partner Support				✓
Executive Sponsor/ Business Planning				✓

SonicWall

Endkunden

Kleine und mittelständische Unternehmen (KMU): SonicWall's TZ-Serie ist besonders beliebt bei KMUs, die zuverlässige und einfach zu verwaltende Firewalls benötigen > Einzelhandel in Österreich

Große Unternehmen und Rechenzentren: Die NSsp-Serie von SonicWall bietet extreme Performance und erweiterten Schutz für große Netzwerke und Serviceprovider

Bildungseinrichtungen & öffentlicher Bereich: Gemeinden, Schulen und Universitäten nutzen SonicWall, um ihre Netzwerke und Daten vor Cyberangriffen zu schützen

Gesundheitswesen: Krankenhäuser und Gesundheitsorganisationen setzen SonicWall ein, um Patientendaten zu sichern und die Compliance mit Datenschutzvorschriften zu gewährleisten

Finanzdienstleister: Banken und Finanzinstitute verwenden SonicWall, um ihre sensiblen Daten und Systeme vor Cyberbedrohungen zu schützen

Einsatzgebiete von Access Management

TD SYNNEX

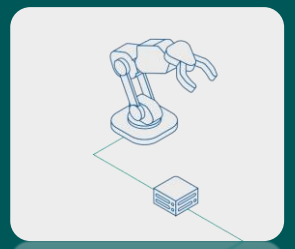
Identitäten absichern, Zugriffe verwalten

Absicherung privilegierter Accounts

User Access auf Netzwerk & Anwendungen via MFA

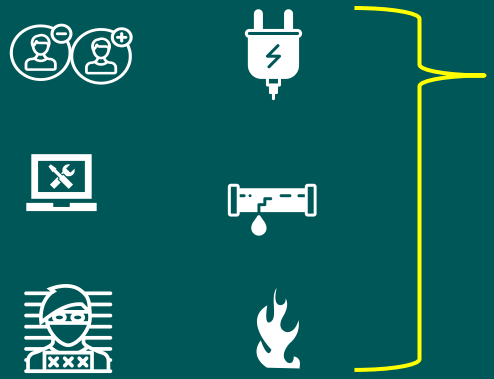
Schutzbedarf mittels Risikobewertung ermitteln

TD SYNNEX



Wie wichtig ist der zu schützende Gegenstand?



+

Welche Bedrohungen gibt es?

+

Welcher Schaden kann entstehen?

+

Die Wahrscheinlichkeit eines Schadens?

⬇

Risikoklassen definieren

3 - 2 - 1 - 0

Häufigkeit des Schadens	5				€€€	
	4					
	3					
	2					
	1					
Problem	Kritisch	1	2	3	4	5
Akzeptabel	Problem					Höhe des Schadens

ÖNORM A7700

RISIKOKLASSE 0	**SEHR HOHES RISIKO** Sehr hoher Schutzbedarf
RISIKOKLASSE 1	**HOHES RISIKO** Hoher Schutzbedarf
RISIKOKLASSE 2	**MITTLERES RISIKO** Mittlerer Schutzbedarf
RISIKOKLASSE 3	**NIEDRIGES RISIKO** Niedriger Schutzbedarf

Risikobewertung lt. BSI
Minimum für Cyber Security Prozesse

TD SYNNEX

	Risikoklasse 3 Geringer Schutzbedarf	Risikoklasse 2 Normaler Schutzbedarf	Risikoklasse 1 Hoher Schutzbedarf	Risikoklasse 0 Sehr hoher Schutzbedarf
Physikalische Sicherheit	Öffentlich	Zugang nur für Befugte	Eintrittskontrolle, verschlossen	Überwachung aller Personen, Sperrzone
Zugriffs- & Rechte-Management	Authentifizierung	Authentifizierung 2 Faktor	• Authentifizierung MFA • Geringste Privilegien (IGM / IAM)	PAM Systeme überwachen alles
Netzwerk, Daten und Kommunikation absichern	Abgrenzung zum Unternehmen (Guest Net)	Netze trennen und APT Schutz	Netze trennen Log Files überwachen, Backup + Fall back	Netze trennen, Log Files überwachen, HA Umgebung, Echtzeit Verteidigung
Überwachung der Sicherheit	Regelmäßige Systemprüfung	Auf Security System Meldungen schnell reagieren	Aktive Überwachung aller Systeme und Datenflüsse	Aktive Überwachung aller Systeme und Datenflüsse + SOC SOAR Team
Prozesse zur Verbesserung der Sicherheit	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung

Identity & Access Management Übersicht

TD SYNNEX

One IDaaS

UA
User Authentication
MFA Multifaktor
Authentifizierung

SSO
Single Sign On

IGA/ IAM
Identity Governance Administration & Identity Access Management

EPM
Endpoint Privileged Management

PAM
Privileged Access Management

Risikoklasse

3

2 — IDEE

AuthN

SpyCloud

MFA, Zero Trust
Phishing Proof

2

Trustelem

IDaaS
Identity as a Service
Cloud native SSO

1

- **OneLogin**
- **Active Roles** (Mid-Market) AD-Management
- **Identity Mgr.** (Enterprise)

OL = Cloud native
IM/AR = on Prem

1

BestSafe

- Prozesse mit Privs versehen/sperren
- Agent based
- Client Schutz auf Prozessebene

0

SafeGuard

3 Produkte

- SPS – SG Privileged Session
- SPP – SG Privileged Passwort
- SPA – SG Privileged Analytics

Bastion

All in One inkl.

- Passwort Vault
- Passwort Manager
- Analytics

Identity & Access Management

TD SYNNEX

PAM: Privileged Access Management

2022 Gartner PAM Magic Quadrant

WALLIX und One Identity werden bei Gartner im Leader Quadrant gelistet (Stand Januar 2022)

Vertrauenswürdig und bewährt

One Identity bietet moderne Identitätslösungen, die angesichts unzähliger menschlicher und maschineller Identitäten (und KI), 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 (IGA), Access Management (AM), Privileged Access Management (PAM) sowie Active Directory Management (AD Mgmt).

80 out of the **Fortune 100** als Kunden

1,000 Partner Auf der Welt

11,000+ Unternehmens-kunden

500M+ Identiäten verwaltet

97% Kunden Zufriedenheit weltweit

20+ Jahre In Identitätssicherheit

ISO 27001 CERTIFIED by schellman

ONE IDENTITY by Quest

Idee

Multifaktor-Authentifizierung MFA, Mobile Authenticator, Secure Access

AuthN by IDEE.

AuthN by IDEE

AuthN verhindert alle Phishing- und Passwort-basierten Angriffe.

Schnellste MFA

- ✓ Einsatz in nur 15 Minuten
- ✓ Plug n Play Integration
- ✓ SAML, OIDC, WS-FED or API

Sicherster

- ✓ Phish-sichere MFA
- ✓ Zero Trust, Zero Knowledge
- ✓ Zero Agents, Zero PII

Von Nutzern geliebt

- ✓ Passwortlos
- ✓ Einzelgerät UX
- ✓ Benutzer entsperrt das Gerät nur

Idee

Multifaktor-Authentifizierung MFA, Mobile Authenticator, Secure Access

Exabeam

SIEM, XDR, Advanced Analytics, Responser, Case-Manager

exabeam™

Real Intelligence.
Real Security.
Real Fast.

Peter Häufel | Director, Channel

Was macht Exabeam einzigartig?

- SIEM Anbieter, seit 5+ Jahren im Leading Quadranten
- 800 MA, Vertrieb lokal in Österreich
- Effizienteste SIEM Lösung am Markt
- Kunden sparen 70% Ihrer Arbeitszeit schon VOR dem KI-Hype
- Innovative Technologie
- On-prem / Hybrid / Cloud-Native
- Als Vollprodukt, aber auch als Erweiterung für andere SIEM Lösungen

exabeam

Was will man mit eine SIEM erreichen?

- Angriffe erkennen, die es durch eine Prävention geschafft haben
- Schnelle, VOLLSTÄNDIGE und EXAKTE Analyse des Vorfalls mit allen beteiligten Usern / Accounts / Devices
- Priorisierung der Vorfälle anhand Ihrer Kritikalität für das Unternehmen
- Detaillierte Vorschläge für Gegenmaßnahmen
- Hilfestellung im Prozess der tiefen Untersuchung
- Ausführen von Gegenmaßnahmen
- Agentic-AI als Turbo voll integriert ohne Kosten

Exabeam beherrscht
die Königsklasse

exabeam

Is this a Threat or legitimate Traffic?

Feb 2 2025 11:49:00 host1 10.78.121.42:350 10.28.161.16:203 up.badsite.local/upload.jar Large outbound traffic volume user=bsalazar winscp.exe

exabeam

Insider Threat Investigation is Too Time Consuming!

- Who owns this asset?
- What is installed on it?
- Is it a business role?
- Any recent changes?
- What host does this IP map to and for how long?
- What user does this IP map to and for how long?

CMDB/Directory Services/Operating System/DHCP

- Is this port opened?
- Is it authorized?
- What is it used for?
- Is this normal traffic behavior?
- Have these hosts communicated with each other using this pattern before?
- What phase in the cyber kill chain (recon) is it?

Traffic Analysis, Ports/Protocols

- What does this alert mean?
- How does it work/what makes it fire?

Alert Details

- Who is this user?
- What is their status?
- What is their role?
- How does their activity compare to their peers/org?
- What privileges do they have?
- What groups do they belong to?
- What is their contact info.?
- Has this user connected to these hosts before?

Directory Services/HRMS

Feb 2 2025 11:49:00 host1 10.78.121.42:350 10.28.161.16:203 up.badsite.local/upload.jar Large outbound traffic volume user=bsalazar winscp.exe

Historical and Current Info.

- How long has this activity occurred?
- What else is happening?
- Is this an approved time period?

DIG

- Where is this going to?

Domain Tools

- What are these hosts names?

Threat Intel

- Is this a known bad actor?
- Have we seen this address accessed by any user/peer group/ the org before?
- What phase in the cyber kill chain (recon) is it?

Machine Learning/Analytics

- Have any of our featured classification algorithms identified this as malicious?
- What is the entropy score for this URL, for the domain?
- Have we seen any user/peer group/the org visit this site before?
- What phase in the cyber kill chain (delivery/payload, C&C) is it?

CVE/Open Source/ Commercial/Internal Intel

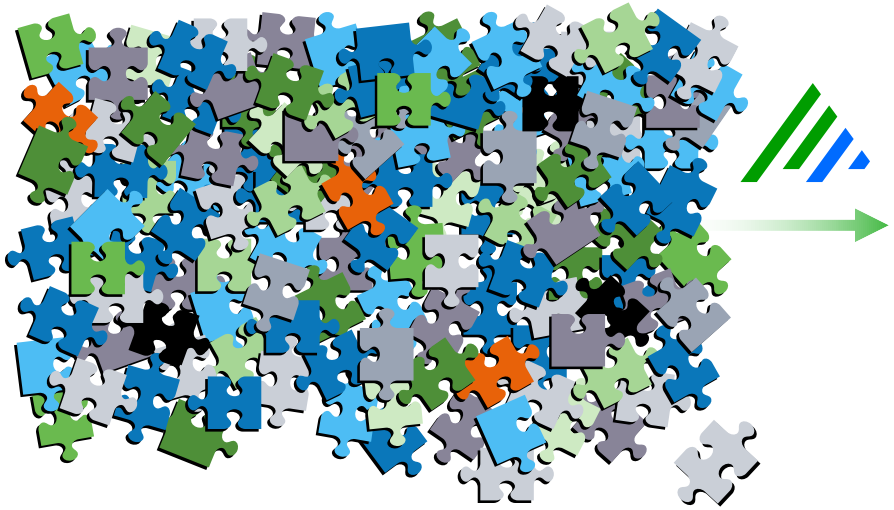
- How new is this domain?
- Is this a known indicator of compromise?
- What is the risk rating/reputation of the domain?
- Is this domain known to serve up malicious content?
- Is this URL being reported as malicious?
- Is this an exploit call or known common exfiltration call?
- What phase in the cyber kill chain (exploit) is it?

Processes

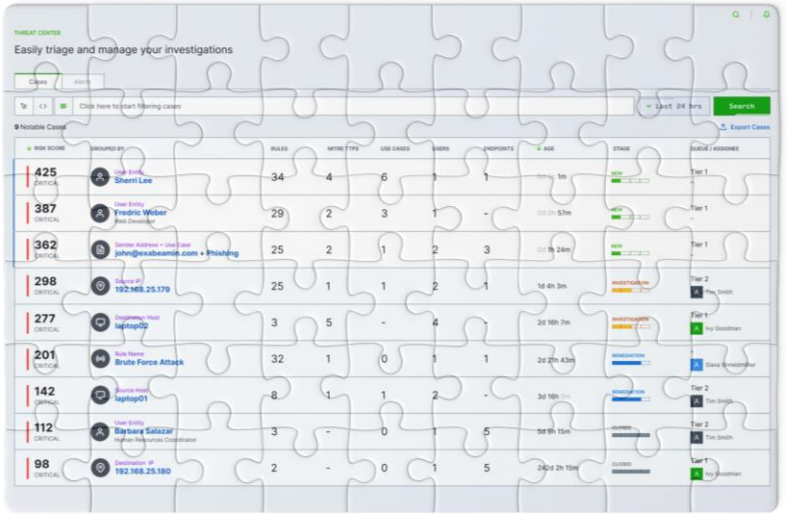
- Is this an authorized process?
- What is it used for?
- Have we seen this before from the user/peer/in the org?
- What is the file hash?
- What phase in the cyber kill chain (install, action/objective) is it?

exabeam

Events and alerts in your log files



Threats Classified via ML Behavior Analysis



Pinpoint high-risk threats with ML Models

Detect complex threats

Prioritize threats

Baseline normal behavior

Follow attacks as they move laterally

exabeam

Example of a MSSP switching to Exabeam

– Onboarding time reduced by 70%

– False Positives reduced by 60%

– Communication with the end customer in an investigation phase reduced by 80%

– MTTA at 9 Minutes

– MTTR at 17 Minutes

– Free up time for analysts by reducing the routine work load

exabeam

Exabeam

Endkunden

Große Unternehmen und Konzerne: Diese Organisationen nutzen Exabeam, um ihre umfangreichen IT-Infrastrukturen zu schützen. Beispiele sind Finanzinstitute, Gesundheitsorganisationen und multinationale Konzerne. Sie profitieren von Exabeams Fähigkeit, große Mengen an Protokolldaten zu verarbeiten und komplexe Bedrohungen zu erkennen

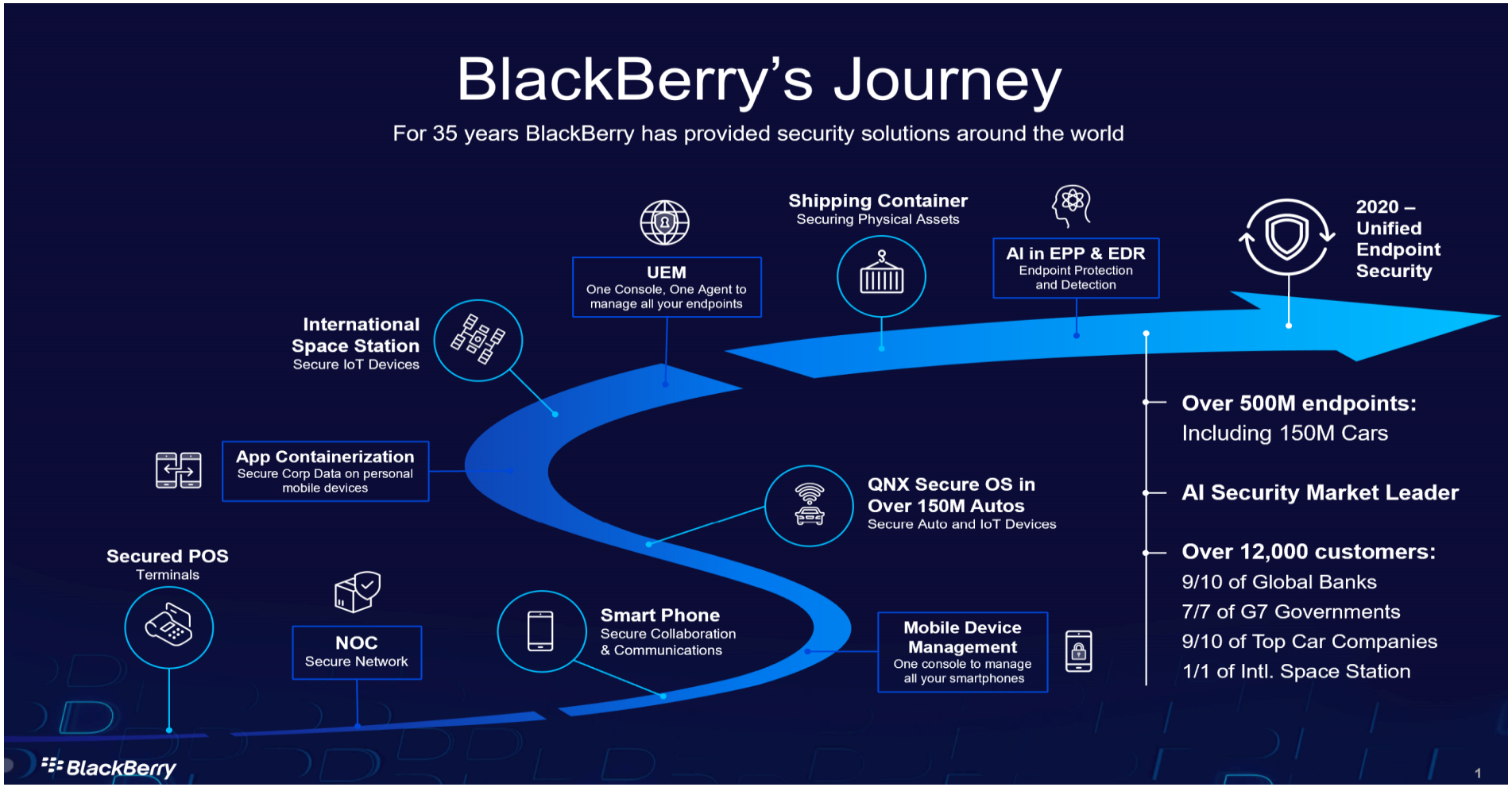
IT-Sicherheitsfirmen: Spezialisierte Sicherheitsunternehmen setzen Exabeam ein, um ihre eigenen Dienstleistungen (SOC-Center) zu verbessern und ihren Kunden fortschrittliche Sicherheitslösungen anzubieten. Diese Firmen nutzen Exabeams SIEM (Security Information and Event Management) und UEBA (User and Entity Behavior Analytics), um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren

Kleine und mittlere Unternehmen (KMUs): Exabeam hilft diesen Unternehmen, ihre Sicherheitsoperationen zu optimieren und effizienter zu gestalten. Sie schätzen die automatisierten Sicherheitsprozesse und die einfache Integration in bestehende Systeme.

Öffentliche Einrichtungen und Regierungsbehörden: Diese Organisationen nutzen Exabeam, um sensible Daten zu schützen und Cyberangriffe abzuwehren. Die Plattform bietet ihnen die Möglichkeit, Bedrohungen in Echtzeit zu überwachen und schnell darauf zu reagieren

Black Berry

Endpoint Management



Globally Recognized for Our Secure and Certified Platform for Critical Communications

Critical Communications

Mobile Fortification

Crisis Management

Education & Cyber-Expertise Development

Black Berry

TD SYNNEX

- **Verhinderung der Abhörung** > Ende-zu-Ende-Verschlüsselung, die mehrere Schichten abdeckt.
- **Verhinderung von Identitätsspoofing** > administrativ verwaltete Konten mit kryptografischen Identitätsnachweisen, ohne öffentliche Benutzerregistrierung.
- **Vermeidung der Metadatensammlung** > kommerzielle und gegnerische Akteure, sodass Sie Ihre Daten kontrollieren.

✓ Verschlüsselungssuite Klassifizierung „streng geheim“ autorisiert
✓ NATO Restricted-Nutzung
✓ Common Criteria Certified
✓ NIAP Compliant Product-Liste
✓ NSA’s CSfC Component-Liste

Dies unterscheidet von kommerziellen Lösungen wie WhatsApp und Signal, die für diplomatische Kommunikation verwendet werden und für Zero-Click-Angriffe anfällig sind.

Black Berry

Endkunden

Große Unternehmen und Konzerne: Diese Organisationen nutzen BlackBerry, um ihre umfangreichen IT-Infrastrukturen zu schützen. Beispiele sind Finanzinstitute, Gesundheitsorganisationen und multinationale Konzerne. Sie profitieren von BlackBerrys Fähigkeit, hochsichere mobile Kommunikation und Endpunktmanagement zu bieten

Sicherheitsfirmen und Managed Security Service Providers (MSSPs): Sicherheitsfirmen und MSSPs setzen BlackBerry ein, um ihren Kunden erstklassige Sicherheitsdienste anzubieten. BlackBerry hilft ihnen, Bedrohungen effizient zu erkennen und darauf zu reagieren, und bietet eine flexible Architektur für die Datenverwaltung

Kleine und mittlere Unternehmen (KMUs): Viele KMUs weltweit nutzen BlackBerry, um ihre Netzwerke und Endpunkte zu sichern. Sie schätzen die automatisierten Sicherheitsprozesse und die einfache Integration in bestehende Systeme. BlackBerry hilft diesen Unternehmen, ihre Sicherheitsoperationen zu optimieren und effizienter zu gestalten

Öffentliche Einrichtungen und Regierungsbehörden: Diese Organisationen nutzen BlackBerry, um sensible Daten zu schützen und Cyberangriffe abzuwehren. Die Plattform bietet ihnen die Möglichkeit,

Lookout

Endpoint Security, Cloud-Security, Zero Trust, Access-Security

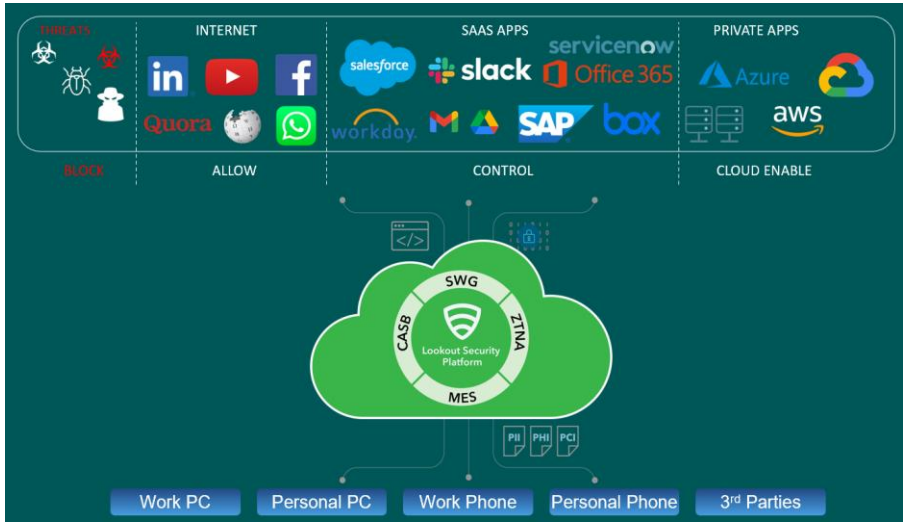
•**Mobile Endpoint Security**: Schutz vor Phishing, bösartigen Apps und Social Engineering-Angriffen.

•**Cloud Security**: Schutz von Daten in SaaS-Anwendungen und cloudbasierten Ablagen.

•**Mobile EDR**: Erweiterte Sichtbarkeit und Reaktionsmöglichkeiten für mobile Bedrohungen.

•**Zero Trust Network Access**: Sicherer Zugriff nur für autorisierte Benutzer und Geräte.

•**Phishing-Schutz**: Spezielle Maßnahmen gegen Phishing-Angriffe, einschließlich Smishing.



Lookout

Endkunden

Große Unternehmen und Konzerne: Diese Organisationen nutzen Lookout, um ihre umfangreichen IT-Infrastrukturen zu schützen. Beispiele sind Finanzinstitute, Gesundheitsorganisationen und multinationale Konzerne. Sie profitieren von Lookouts Fähigkeit, mobile Endgeräte und Daten umfassend zu sichern

Managed Security Service Providers (MSSPs): MSSPs setzen Lookout ein, um ihren Kunden erstklassige Sicherheitsdienste anzubieten. Lookout hilft ihnen, Bedrohungen effizient zu erkennen und darauf zu reagieren, und bietet eine flexible Architektur für die Datenverwaltung

Kleine und mittlere Unternehmen (KMUs): Viele KMUs weltweit nutzen Lookout, um ihre Netzwerke und mobilen Endpunkte zu sichern. Sie schätzen die automatisierten Sicherheitsprozesse und die einfache Integration in bestehende Systeme. Lookout hilft diesen Unternehmen, ihre Sicherheitsoperationen zu optimieren und effizienter zu gestalten

Öffentliche Einrichtungen und Regierungsbehörden: Diese Organisationen nutzen Lookout, um sensible Daten zu schützen und Cyberangriffe abzuwehren. Die Plattform bietet ihnen die Möglichkeit, Bedrohungen in Echtzeit zu überwachen und schnell darauf zu reagieren

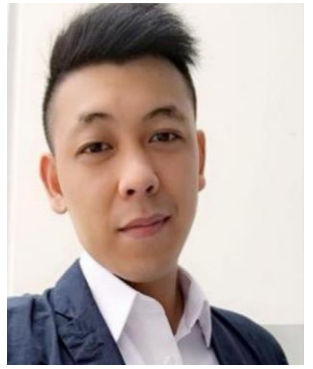
Security - Team Austria

security.at@tdsynnex.com

Raluca Zupcec
Business Unit Manager
+43 676 847 774 319

Cristina-Maria Babu
Sales Specialist
+43 1 48801 774

Niloofar Sharbafian
Sales Specialist
+43 1 48801 802



Michael Uy-Oco
Sales Specialist
+43 676847774311

Johannes Föger
Business Development Manager
+43 676 847774306

Wolfgang Rieger
Business Development Manager DACH
Mobil: +49 175 7270279

Arik Seils
Business Development Manager DACH
arik.seils@tdsynnex.com

Das Security Portfolio von TD SYNNEX

TD SYNNEX hilft Ihnen die Komplexität effektiver Cyber-Security-Lösungen zu reduzieren und erfolgreich umzusetzen.

Kernkompetenzen

- SIEM/SOAR/ATO
- MFA/PAM/IAM
- MOM/Mobility/Endpoint & Cloud Security
- Netzwerk-/lnfrastruktur-/Industrial-Security

Wir unterstützen Sie mit

- Vulnerability Management & Asset Management Service
- Managed Authentication & Identity Service
- Security Managed Services (Firewall/ID/Mobile/IAM/PAM)
- Managed SOC/MOR/XOR Service
- Security Themen in der TD SYNNEX Academy
- Top Cyber-Sicherheitslösungen und Services
- Kompetente Unterstützung für sichere Umsetzung von Digitalisierung und loT-Projekten
- Ganzheitliches IT-Security-Vertriebskonzept
- Marketing Unterstützung um Märkte zu entwickeln
- TD SYNNEX Acadamy

Ausführliche Informationen erhalten Sie bei den Security-Spezialisten der TD SYNNEX per E-Mail an security.at@tdsynnex.com.

Security & Mobility Hersteller Portfolio Auszug:

exabeam · IBM · Lookout · Microsoft · BlackBerry · vmware · SONICWALL · Barracuda · Cisco Distributor · paloalto NETWORKS · IDEE · ONE IDENTITY · secunet · SpyCloud · wallix · ProLion · HPE aruba networking

Über die BBG (Bundesbeschaffung GmbH):

LOGPOINT · STACKIT