TD SYNNEX | Services

OXFORD COMPUTER GROUP

„Hacker schlafen nie“

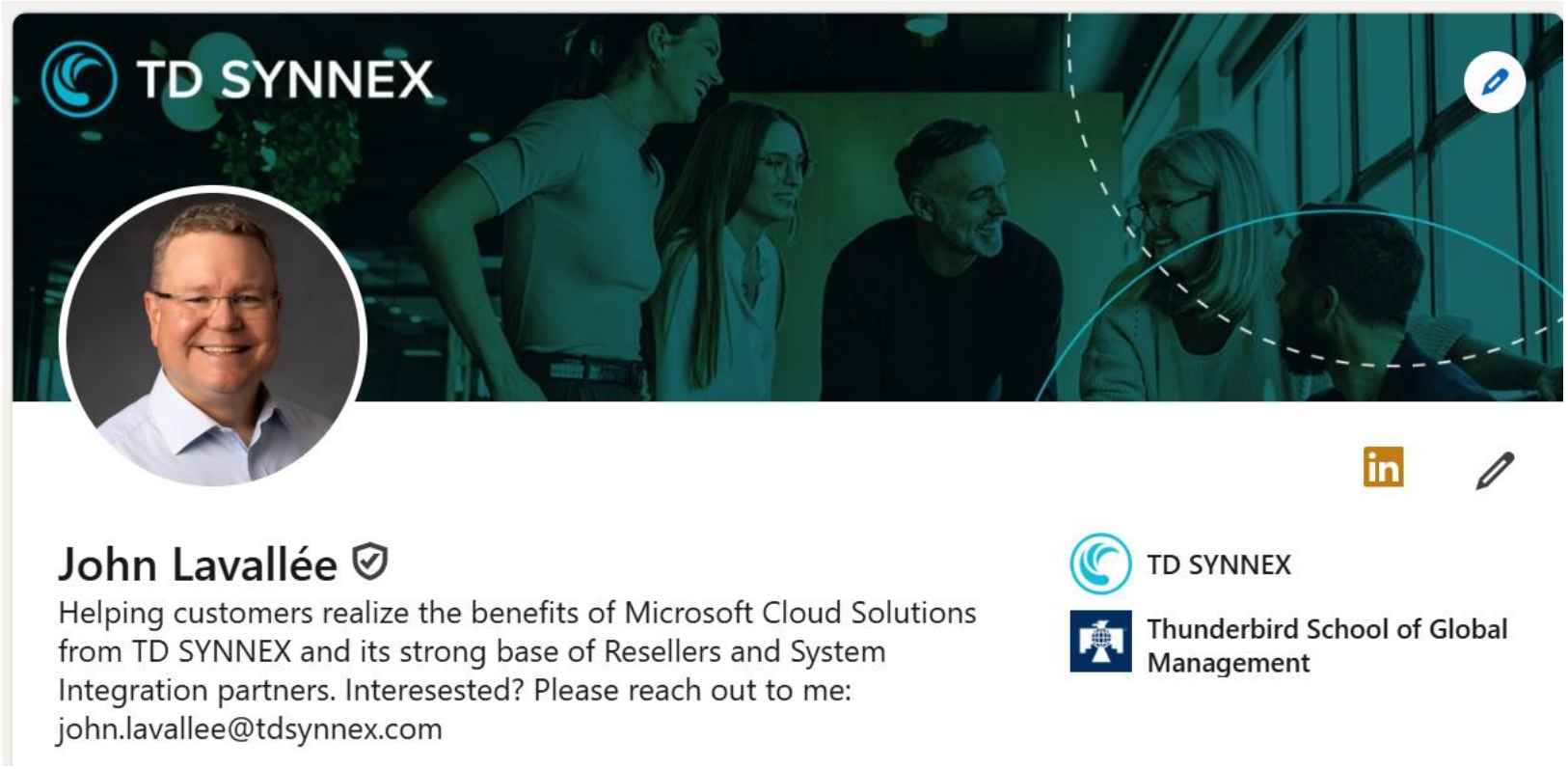
Warum IT-Überwachung rund um die Uhr unerlässlich ist

OXFORD COMPUTER GROUP
16. Security & Efficiency Summit 2025

05. September 2025
Stadthalle Erding

Über mich

TD SYNNEX



https://www.linkedin.com/in/john-lavallée/

Business Development Manager – Microsoft Cloud & SAP Solutions

TD SYNNEX | Microsoft

Über uns

Wir sind 23.500 der besten und klügsten Köpfe der IT-Branche, die eine ungebrochene Leidenschaft dafür teilen, der Welt überzeugende Technologieprodukte, Dienstleistungen und Lösungen zu bieten.

Wir sind ein innovativer Partner, der unseren Kunden hilft, den Wert ihrer IT-Investments zu maximieren.

5,000+
Cloud skilled co-workers

100+
Countries served

150,000+
Customers

$3bn
Aggregation cloud marketplace

Microsoft
2023 Partner of the Year

Winner
Operational Excellence Award
Finalist
Indirect Provider Award
Device Partner Distributor/Reseller Award

Country Partner Of The Year – Ecuador
Country Partner Of The Year – Cayman Islands
Country Partner Of The Year – Trinidad y Tobago
Indirect Partner Of The Year – Switzerland

Microsoft
Solutions Partner

TD SYNNEX Microsoft Team & Unterstützung für unsere Partner!

Channel Marketing Team

Anna Anstett
Channel Marketing Manager

Sami Karra-Batak
Channel Marketing Manager

Carolin Friedl
Channel Marketing Manager

Center of Excellence

Tiago Fernandez
Director Hybrid Cloud

Martin Roselieb
SAP on Azure Solution Architect

Benedikt Pichotka
Business Unit Director Cloud

Innendienst

Britta Anders
Teamlead Innendienst

Robbert Biben
Customer Success Manager

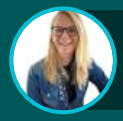
Sonja Keller
Internal Sales Microsoft

Georg Jakob
Customer Success Manager

Oliver Adomeit
Internal Sales Microsoft

Sarah Vollmer
Customer Success Manager

Jan Uwe Morrone Merrone
Internal Sales Microsoft

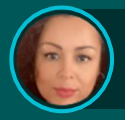


Nicola Schmidt
Customer Success Manager

Patricia Gressley
Internal Sales Microsoft

Christiano Neves
Telesales

Dominik Rembold
Customer Success Manager



Denise Tomann
Internal Sales Microsoft Onprem

Außendienst

Alexander Richter
Teamlead Cloud Business Development

Patrick Theijs
Business Development Manager

Andreas Wolffs
Business Development Manager

Mark Dustin Wilms
Business Development Manager

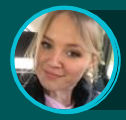
Dennis Heinrich
Business Development Manager

Christian Oeckerath
Business Development Manager

Marina Vlasova
Business Development Manager

Ferdinand Velte
Business Development Manager

John Lavallée
Business Development Manager



Anastasia Andreeva
Business Development Manager - Copilot

Microsoft Business Management

Jola Hysko
Business Manager Cloud

Claudia Naumann
Business Manager OEM/FPP/ESD

Technical Services & Solutions

Frank Siepmann
Teamlead Presales

Natascha Berger
Technical Specialist

Andreas Andorfer
Technical Specialist

Arik Seils
Technical Specialist
Technical Presales

Services

Christian Borutta
Business Development Manager Services

Sebastian Haubner
Platform Lead

Die **Bedrohung** im Cyberraum ist so hoch wie nie zuvor **Ransomware** ist und bleibt die größte Bedrohung

BSI - Die Lage der IT-Sicherheit in Deutschland (bund.de)

Die Lage der IT-Sicherheit in Deutschland 2024

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland informiert das BSI jährlich über die Bedrohungslage im Cyberraum. Im Bericht für das Jahr 2024 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.

Typische Zeiten für Cyberangriffe

- **Freitag nachmittags & am Wochenende:**
  - Weniger Personal, langsamere Reaktion.
- **Feiertage:**
  - Geringere Wachsamkeit.
- **Nachtstunden:**
  - Weniger Überwachung und verzögerte Erkennung.
- **Bei wichtigen Ereignissen:**
  - Fusionen, Börsengängen oder Krisen.

CYBERSICHERHEIT

18.03.2022, 10:52 Uhr

Cyberattacke auf Stephansdom: Hacker lassen nachts Glocken läuten

Mitten in der Nacht: ohrenbetäubender Lärm aus dem Stephansdom in Wien. Hacker nutzten eine Fernwartungsverbindung einer Glockenfirma. Die Attacke weckte ungute Assoziationen.

Cyberattacke auf en Stephansdom in Wien: Plötzlich läuteten die Glocken. panthermedia.net/babenkodenis

Plötzlich läuteten im Stephansdom in Wien die Glocken, mitten in der Nacht. Viele Wiener waren sofort in Alarmbereitschaft, als gegen 2 Uhr am Morgen das Geläut losging. Brennt es? Ist jemand gestorben? Ist etwa Krieg ausgebrochen?

Tatsächlich ist in diesen Tagen die Assoziation leider nachvollziehbar: Die ukrainische Grenze ist knapp 600 Kilometer entfernt, der Krieg, den Russlands Präsident Wladimir Putin dort angezettelt hat, tagtäglich Thema auf der ganzen Welt.

Hackerangriff auf Stephansdom in Wien: Offene Ports in der Firewall

Schnell war klar: Ein Hackerangriff steckt hinter dem nächtlichen Läuten. 20 Minuten lang läuteten die Glocken im Stephansdom, dann konnte Dompfarrer Toni Faber mit seinem eigenen Computer eingreifen und für Ruhe sorgen. „Wir entschuldigen uns bei allen, die dadurch geweckt wurden“, sagte ein Sprecher der Erzdiözese Wien.

Kleine- und Mittlere Unternehmen

Informationen und Hilfestellungen für KMU

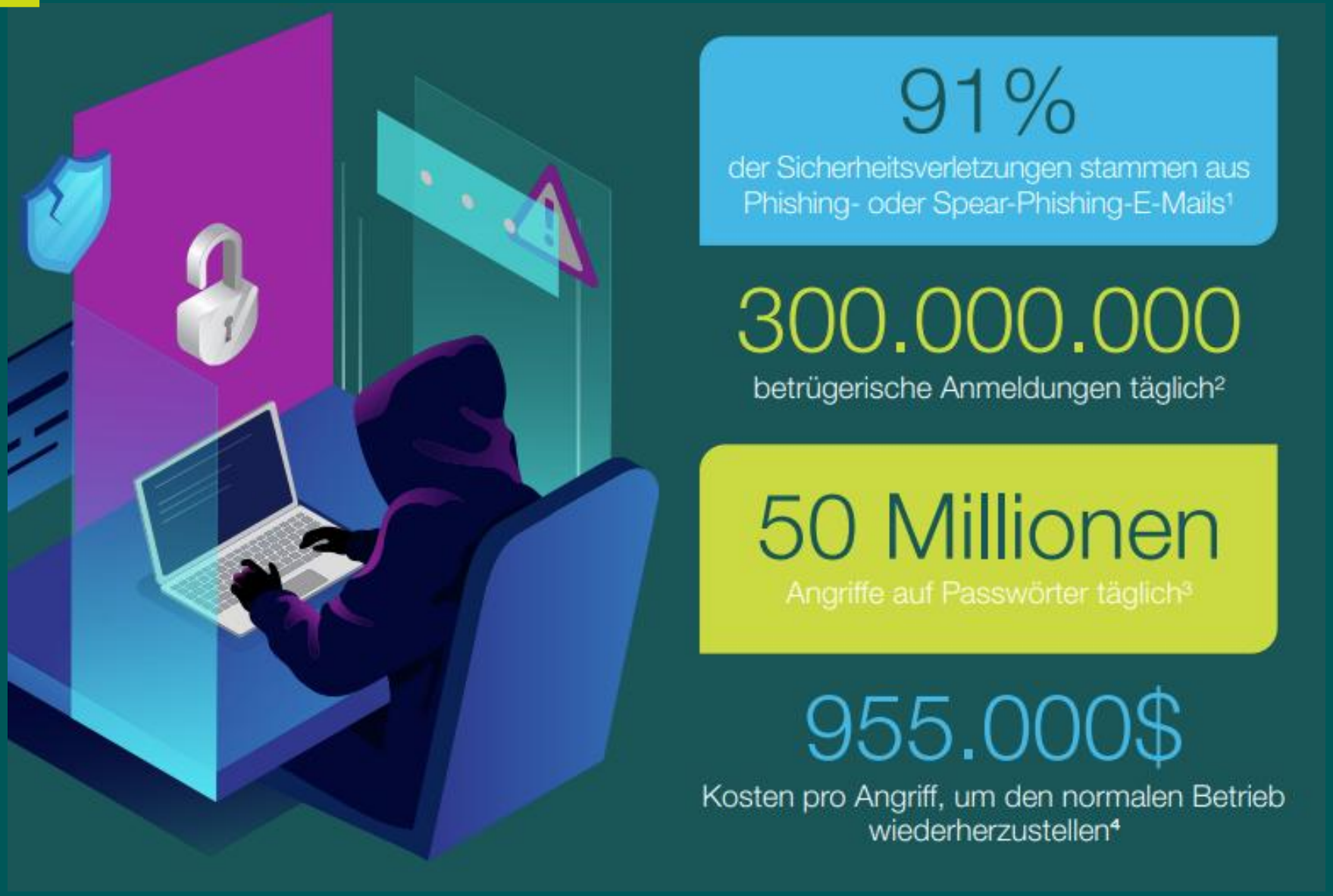
Kleine und mittlere Unternehmen (KMU) werden zunehmend Ziel von Cyber-Attacken. Nicht selten führen diese zu immensen Schäden und schwächen die Unternehmensreputation. Oftmals werden Daten von Kunden und Kooperationspartnern sowie andere sensible Daten abgegriffen, verändert, gelöscht, verschlüsselt und/oder auf inkriminierten Internetseiten veröffentlicht. Wiederholt nutzen Kriminelle die gestohlenen Daten für weitere Hackerangriffe und andere Straftaten.

Dabei werden KMU meist nicht zielgerichtet zum Opfer, sondern werden von großflächig und automatisiert durchgeführten Angriffen getroffen. Es ist also höchste Zeit auch für KMU, die Informations- und Cyber-Sicherheit auf den neuesten Stand zu bringen und Mitarbeiterinnen und Mitarbeiter beim Gebrauch der Informationstechnik (IT) im Hinblick auf die gängigen Betrugsmaschen der Hacker regelmäßig zu sensibilisieren.

Auf diesen Seiten gibt das BSI ausgewählte hilfreiche Tipps - für Unternehmen ohne IT-Expertise und für Unternehmen, die sich bereits eigene oder extern beauftragte IT-Fachleute leisten.

Einige erstaunliche Statistiken !

TD SYNNEX

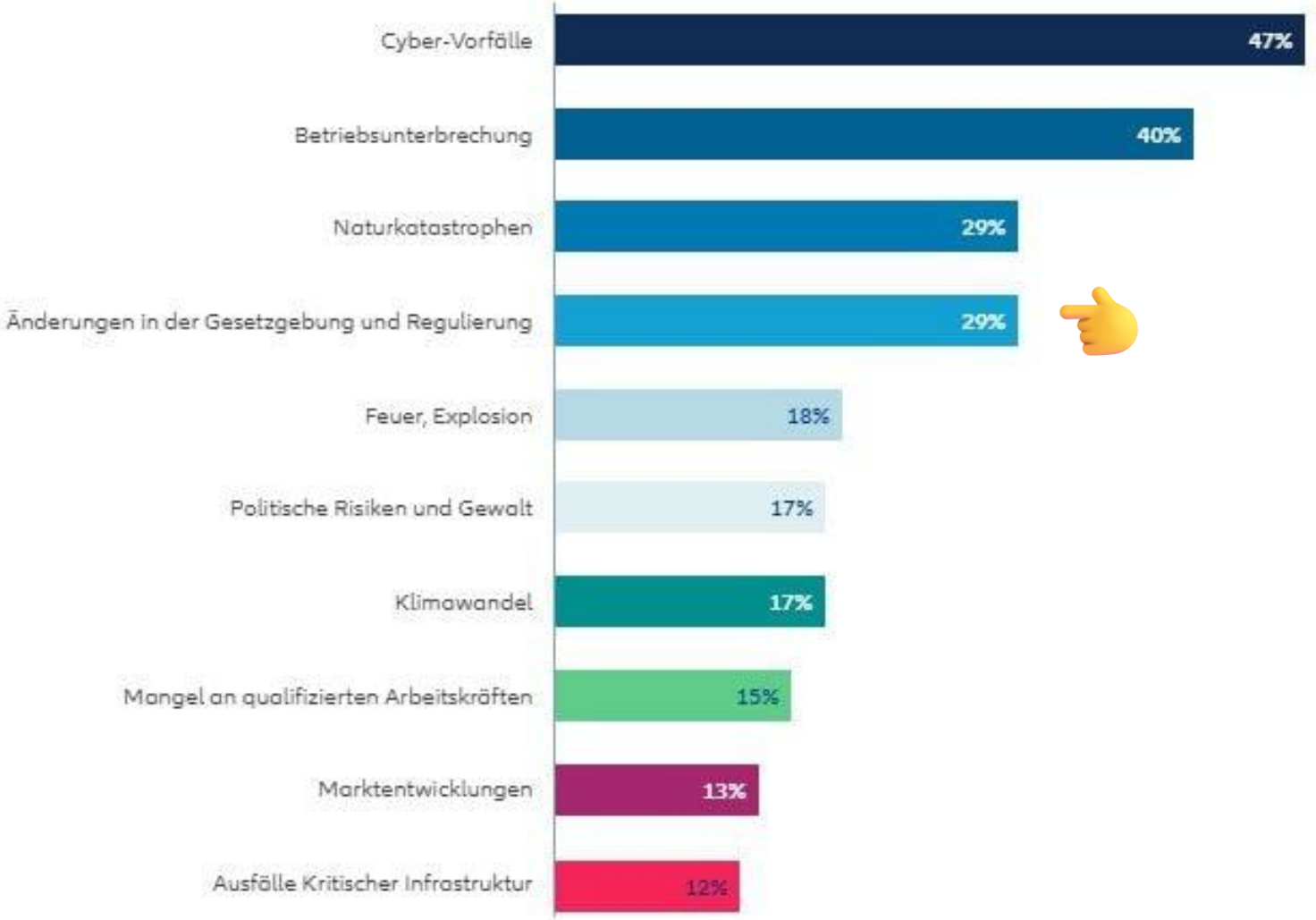


Allianz

Top 10 Geschäftsrisiken in Deutschland im Jahr 2025

Allianz Risk Barometer 2025

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 451. Die Zahlen ergeben nicht 100 %, da jeweils bis zu drei Risiken ausgewählt werden konnten.

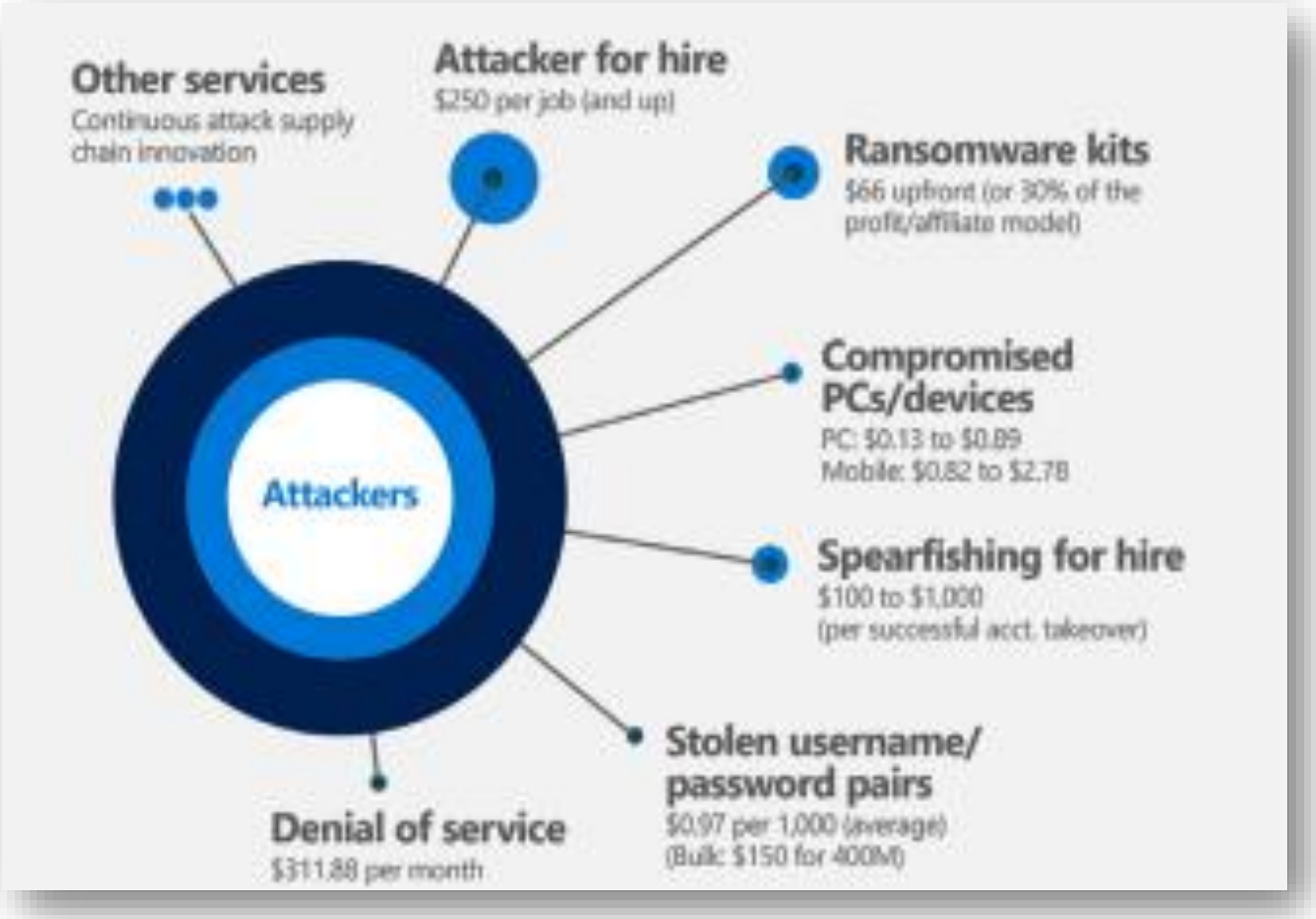


Allianz Commercial News & Insights

Quelle: Allianz Commercial

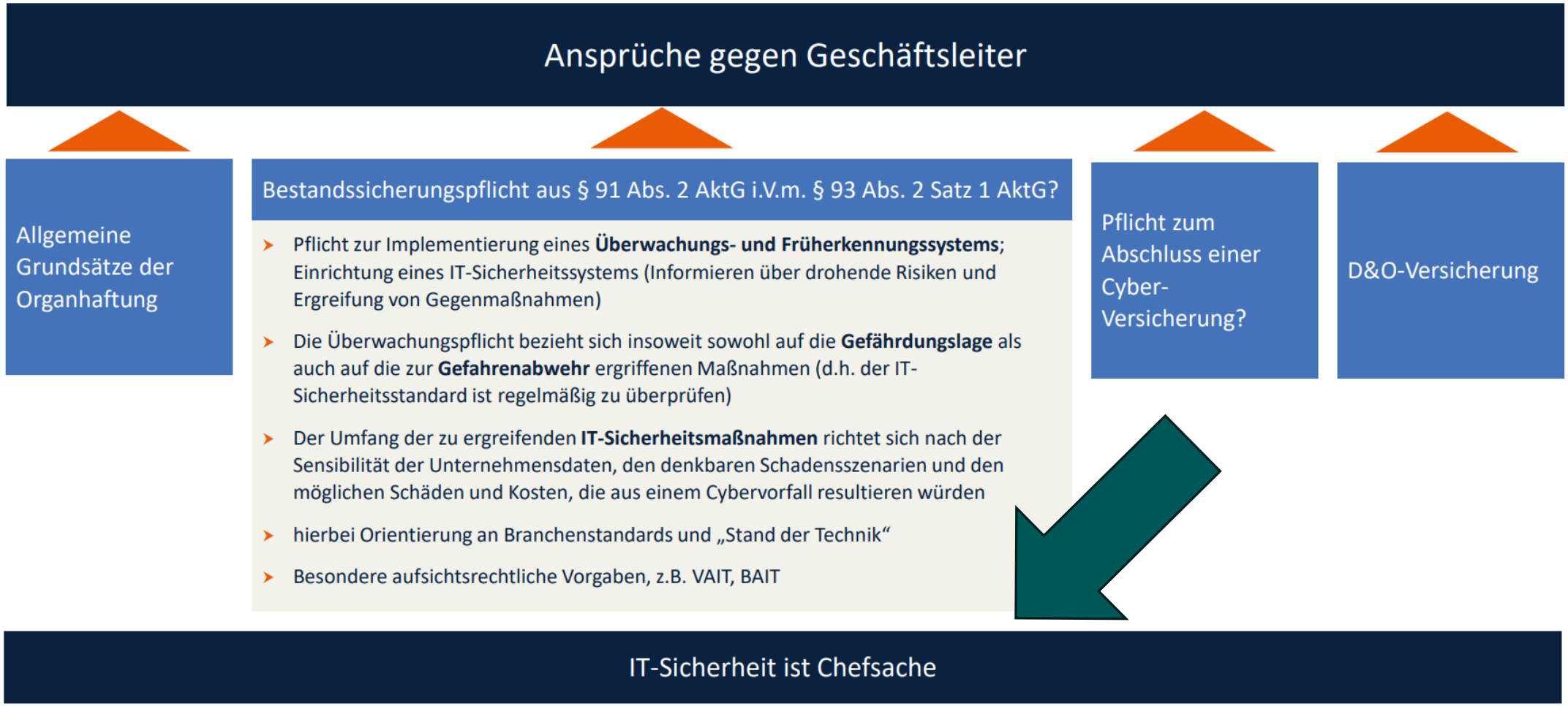
Die zunehmende Häufigkeit erpresserischer Ransomware-Angriffe und die steigenden Kosten von Datenschutzverletzungen **(4,35 Mio. US-Dollar!)** machen Cyberrisiken zu einer akuten Bedrohung.

Preise zum Kauf stehender Cybercrime-Dienste



- Angreifer mieten – ab €200
- Ransomware Kits - €60 im Voraus (oder 30 % des Gewinn-/Affiliate-Modells)
- kompromittierte PCs/Geräte – PC €0,12 bis €0,80 / Handys €0,80 bis €2,50
- Spear-Fishing - €100 - €1.000
- gestohlene Benutzername/Passwort-Paare - €0,97 für 1.000 (durchschnittlich) oder €150 für 400 Mio.
- Denial of Service - €280 pro Monat
- Andere Dienste - Kontinuierlicher Angriff auf Innovationen in der Lieferkette

Ansprüche des betroffenen Unternehmens



Quelle: https://www.jura.hhu.de/fileadmin/redaktion/Fakultaeten/Juristische_Fakultaet/IVR/Forum_Versicherungsrecht/Sieg_-_Cyberrisiken_-_Haftungsszenarien_fuer_betroffene_Unternehmen.pdf

Wenn Sie denken, dass Hacker beängstigend sind, sollten Sie einmal die NIS2-Verordnung lesen!

TD SYNNEX

TD SYNNEX | Services

Also….wie bin ich bestens vorbereitet und geschützt?

Mit einem SOC – Security Operations Center!

Was ist ein SOC? Eine zentrale Einheit innerhalb eines Unternehmens oder einer externe Organisation, die sich mit der:

Überwachung
Analyse
Reaktion auf IT-Sicherheitsvorfälle beschäftigt.

TD SYNNEX | Services

Was ist ein SOC (Security Operations Center)?

Tools

Asset discovery
SIEM (Security Incident & Event Management)
XDR (Extended Detection Response)
SOAR (Security Orchestration, Automation, and Response)
Vulnerability Assessment
Behavioural monitoring
GRC (Governance, Risk Mgt., Compliance)

In-house Average cost: E500k / y

1

People

Security analysts
Security engineer
Security Manager
CISO (Chief Information Security Officer)
IR (Incident Response) Team
Director IR
Director Threat Intel

In-house Average cost: 24/7 engineers + team E1M / y

2

Process

Classify and Triage events
Prioritize and Analyze
Remediation and advisory steps
Assessments and review
Compliance

In-house Average time to be fully up and running: 3 years

3

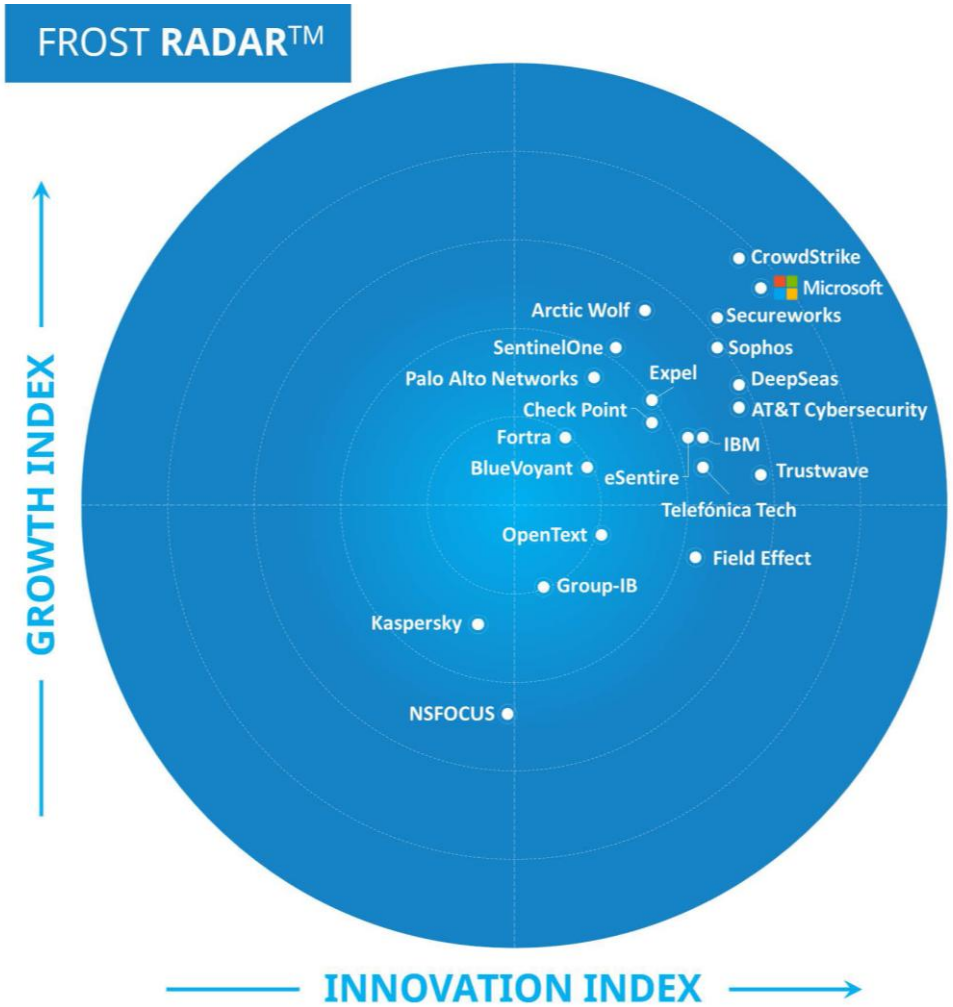
Wie hilft Microsoft?

"Microsoft is already making waves as one of the most innovative in the space."*

*Frost & Sullivan, Frost Radar™: Managed Detection and Response, 2024, Lucas Ferreyra, March 2024.

FROST RADAR™

Managed Detection and Response (MDR) 2024



Microsoft helps organizations secure their future

#1
Modern Endpoint Vendor in the market [1]

15K+
Partners in Microsoft Security Ecosystem

135M
Devices managed by Microsoft Security solutions [2]

Proven Technology

Gartner FORRESTER IDC

Leader in 18
Gartner, Forrester, IDC reports

Microsoft Investment

34k
Engineers working on Security

$20B
Spent on Research and Development

Profitability

60%
Up to 60% margin on Microsoft Security

60%
Savings potential for customers using Microsoft ME5 [3]

1 IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment (doc #US50521223, January 2024.
2 Microsoft Digital Defense Report, 2023
3 Savings based on publicly available estimated pricing for other vendor solutions and web direct/base price shown for Microsoft offerings. Price is not guaranteed and subject to change.

Microsoft Security Overview

Secure and govern data

Reduce the risk of sensitive data leak, data oversharing, and non-compliance

Microsoft Purview

Govern access

Monitor overprivileged and risky users in real-time

Microsoft Entra ID

Manage device estate

Mitigate risk of personal / unsecured or unmanaged devices

Microsoft Intune

Secure all AI apps usage

Discover shadow AI application landscape and secure sensitive information in them with a CASB

Microsoft Defender for Cloud Apps

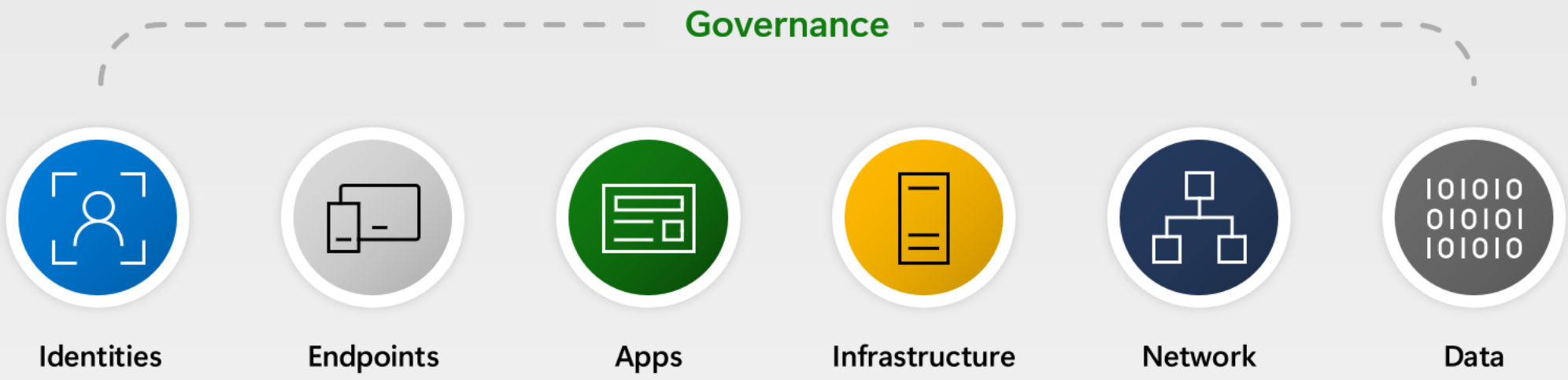
Supercharge threat protection

Get unified visibility, investigation, and response, across the digital estate

Microsoft Defender for Identity & Endpoints

An integrated solution built on the Microsoft 365 security suite. This play helps organizations defend against evolving threats by providing protection across attack vectors and automating threat response.

Zero Trust ++


Governance
Identities
Endpoints
Apps
Infrastructure
Network
Data
Threat protection
Advanced Data Security
Security Operations Management

TD SYNNEX | Services

Ein effektives Managed Detection & Response (MDR) Lösung

Response
SOAR
AI for the SOC analyst
Playbooks
Incident Response

Threat Hunting
Proactive – Hypothesis, HVA
Reactive – Speed and Scale
Search Everywhere

Detection
EDR / SIEM – Avoid False Positives
Threat Analytics
Sandbox
Machine Learning

Monitoring
24x7 Human Monitoriing
UBA / UEBA
Telemetry
Data Lakes

chorus

chorus ist einer von knapp 60 MXDR-Lösungspartner Weltweit!

chorus

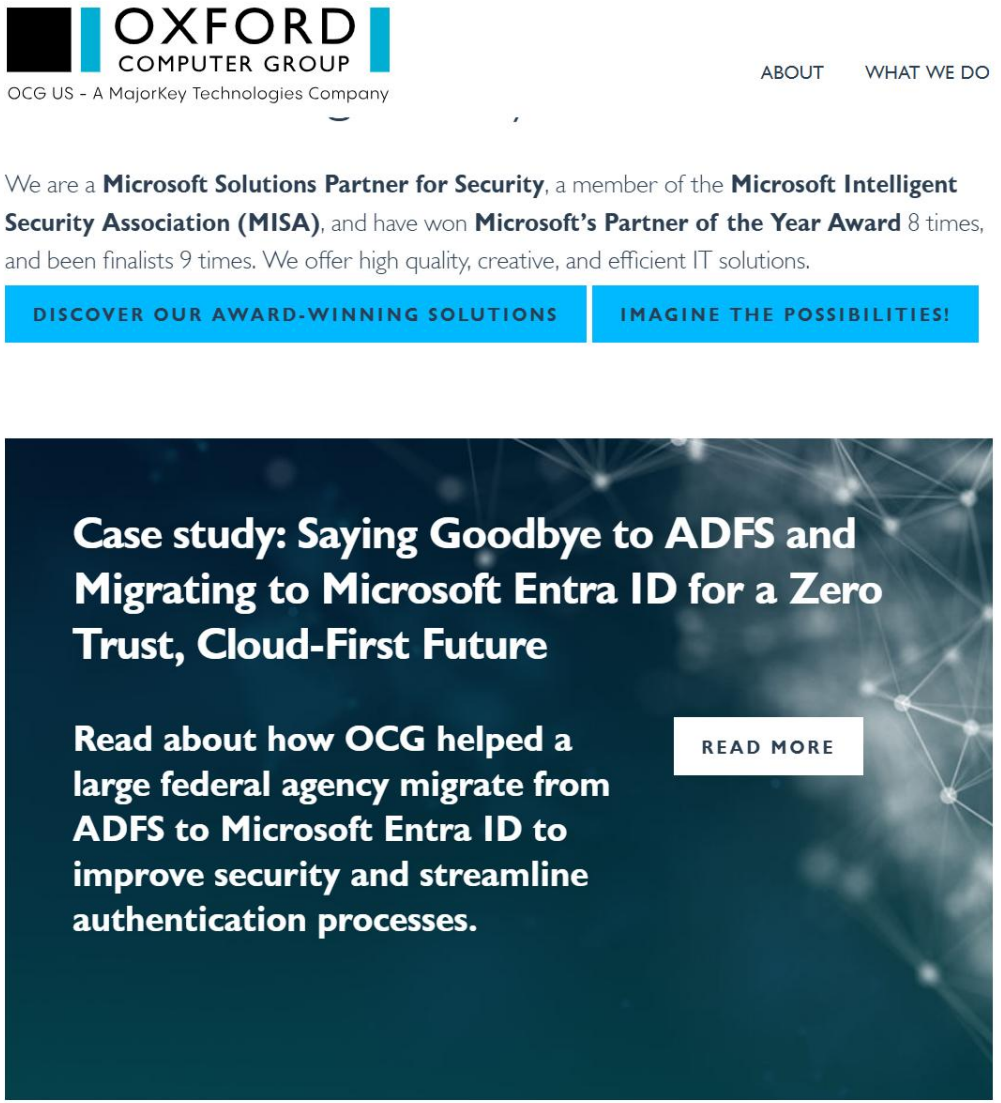
- MXDR-Partner: geprüft & spezialisiert von Microsoft
- Top-Security-Know-how
- Lösungen für M365 Defender & Sentinel
- Global verfügbar
- Proaktiver Schutz vor Cyberbedrohungen

TD SYNNEX | Services

Ihr Hauptansprechpartner?

OXFORD COMPUTER GROUP

- Starten Sie mit einem (kostenlosen) Microsoft Security Assessment
- Lücke erkennen und mit OXFORD COMPUTER GROUP einen Plan machen.
- Beste Sicherheit mit SOC-erfüllen



Noch Fragen? - SOC as a Service