

Sicherheit statt falscher Zauber: Wie *Managed SASE* zum Wettbewerbsvorteil wird



MEET SWISS INFOSEC!

23. Juni 2025, Radisson Blu Hotel, Zürich Flughafen



Kurze Vorstellung



Daniel Marthaler
Senior Cybersecurity Architect
Consulteer InCyber



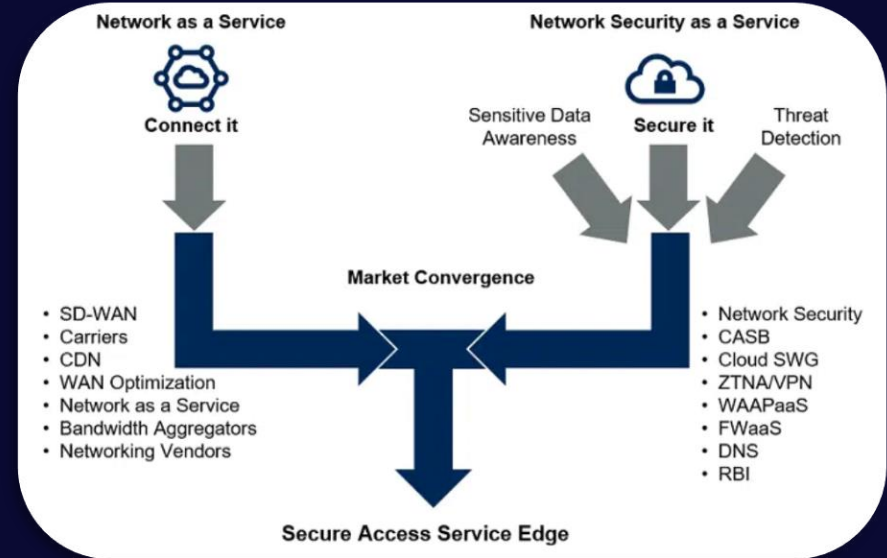
Jürgen Hofmann
Channel Sales Engineer
Cato Networks



CATO
NETWORKS

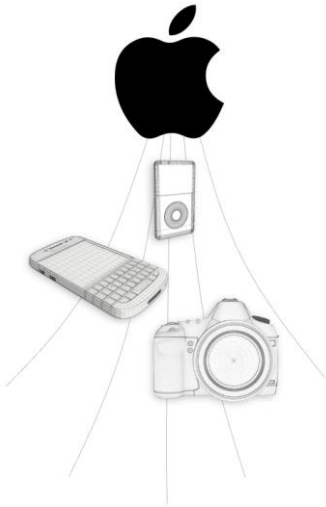
Was ist SASE?

- Vereint Netzwerk- und Sicherheitsfunktionen in einem Service
- Vereinheitlicht Schutz für alle Edge-Typen
- Cloudnative Architektur mit globaler Skalierbarkeit
- Ermöglicht Zero-Trust-Zugriff auf Identitätsbasis
- Echtzeit-Sicherheitskontext und Compliance-Richtlinien



Transformation durch Konvergenz & Abstraktion der Komplexität

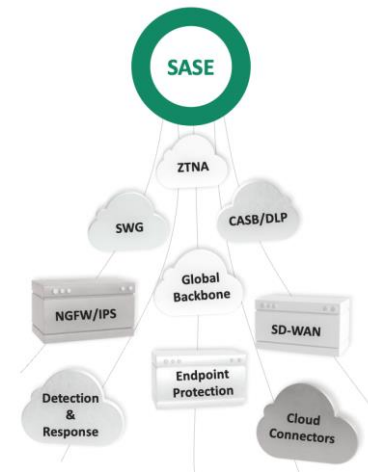
PRODUCTIVITY EVERYWHERE



AGILE COMPUTE & STORAGE



SECURE & OPTIMIZED BUSINESS

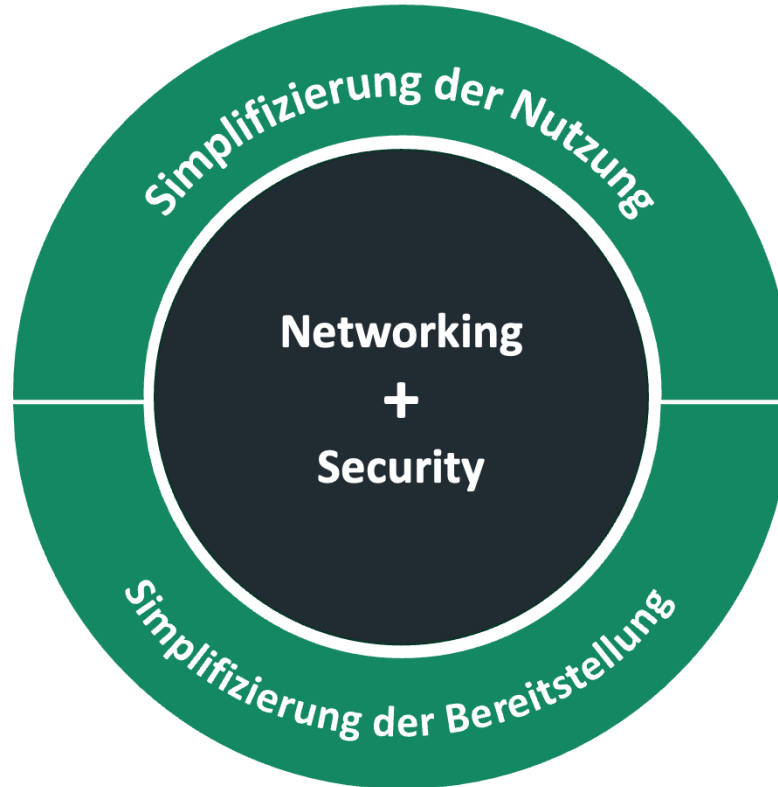


After decades of focusing on network **performance and features**, future network innovation will target **operational simplicity, automation, reliability** and **flexible** business models.

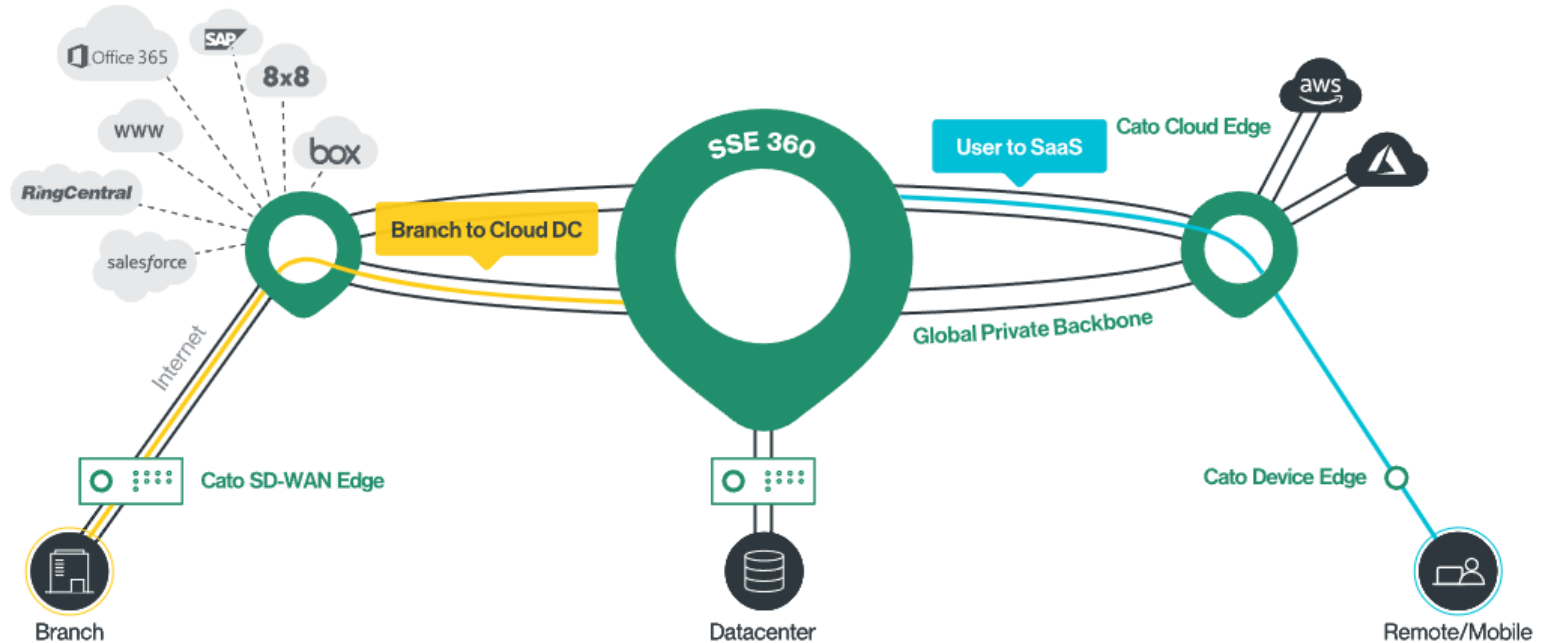
Gartner®

Strategic roadmap for networking 2019

Das Versprechen von SASE



Cato SASE Cloud Plattform



Radikale **Simplifizierung** des Netzwerk- und Sicherheitsinfrastrukturbetriebs durch einen **Plattformansatz** anstelle von separaten Lösungen.

Dies führt zu **geringeren Kosten, weniger Komplexität und höherer Effizienz.**

Komax

- Starre Legacy-Netzwerke behinderten Cloud-Migration
- Unsicherer Remote-Zugriff für globale Teams
- Hohe Betriebskosten durch manuelle Konfiguration
- Fehlende Transparenz über Datenflüsse



Swissport

- Fragmentierte Sicherheitstools an 300 Standorten
- Compliance-Risiken durch uneinheitliche Policies
- Ineffizientes Netzwerk-Design für Flughafen-Operations
- Langsame Reaktion auf Sicherheitsvorfälle

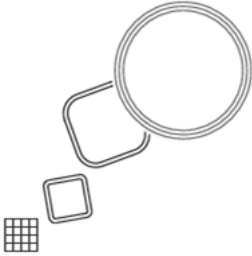


Haefele

- Ransomware-Angriff legte weltweite Standorte still
- Veraltete Sicherheitsarchitektur ohne Zero Trust
- Hohe MPLS-Kosten und komplexe Netzwerkverwaltung
- Langsame Cloud-Performance für Microsoft 365



Evolutionärer Ansatz



MPLS migration to SD-WAN



Optimised Global Connectivity



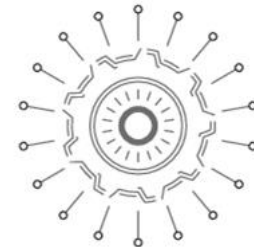
Secure Branch Internet Access



Cloud Acceleration and Control

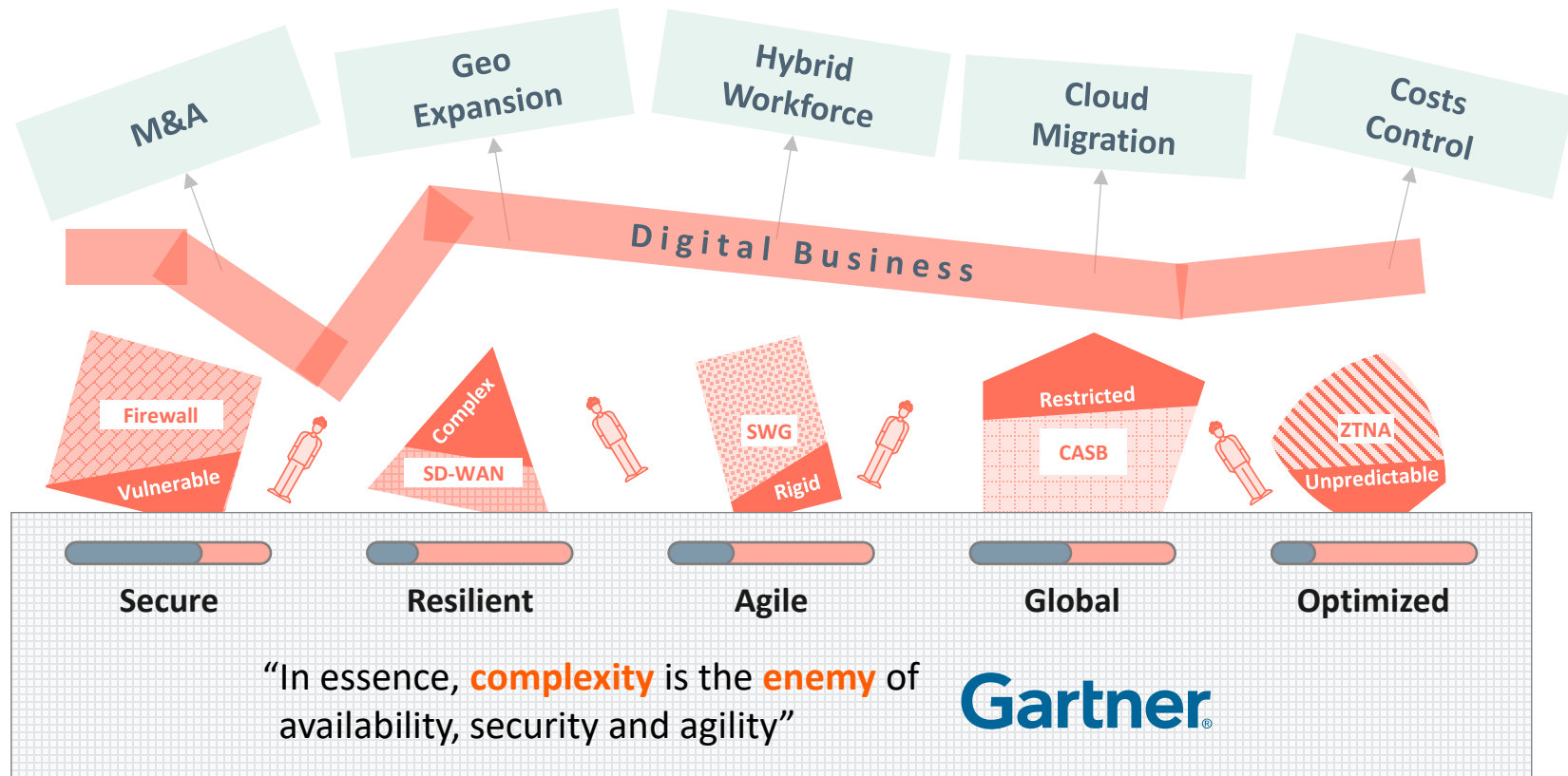


Remote Access and Optimisation

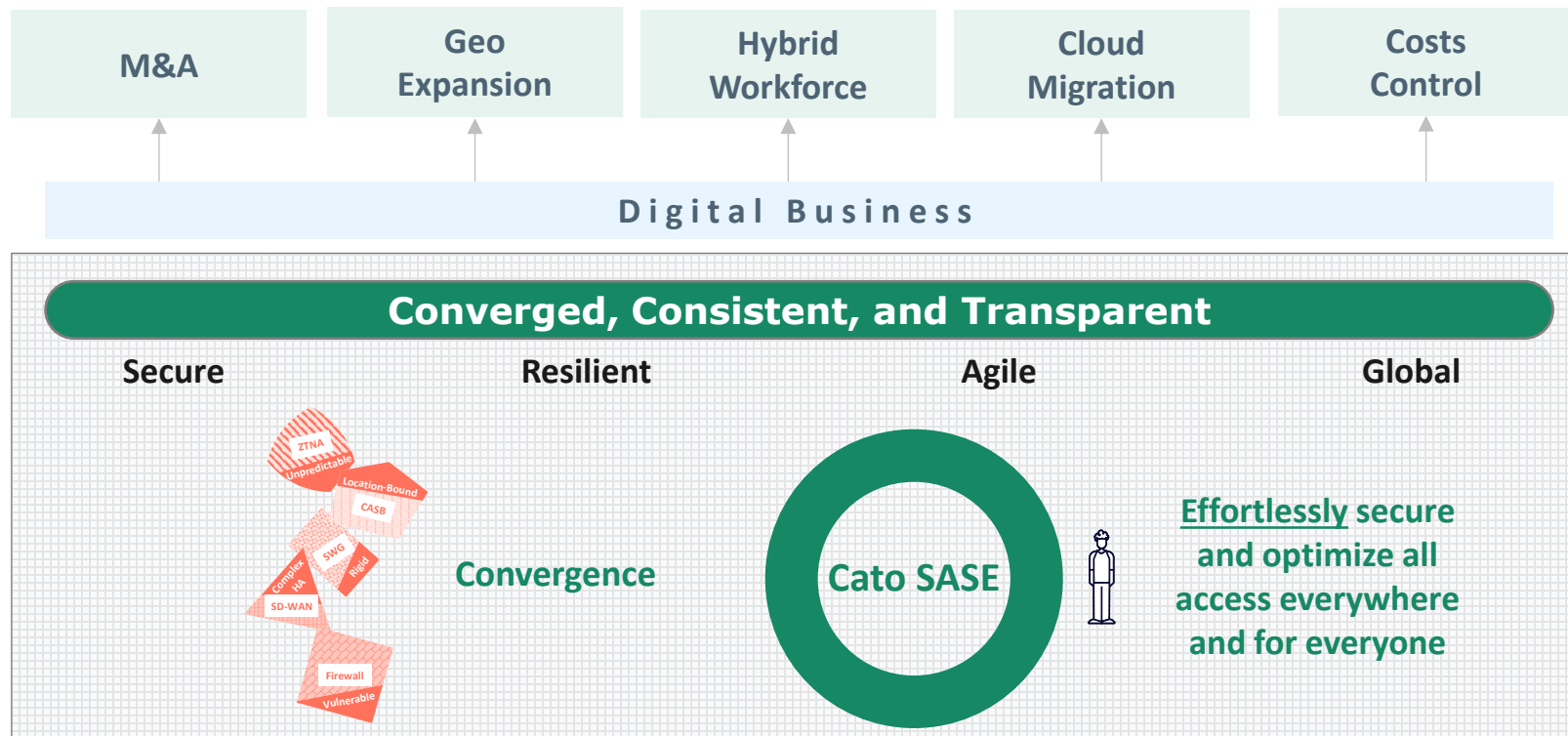


Single Management

Die falsche IT-Plattform bremst das digitale Geschäft



Die Plattform, um digitales Geschäft voranzutreiben



Managed SASE



BASE SERVICE

7x24 Global Support

Rund um die Uhr verfügbar,
genau dann, wenn Sie
Unterstützung benötigen.



SERVICE OPTIONS

- Configuration Management
- Customer Success Engineer

Definieren Sie den
Leistungsumfang selbst –
Sie haben die Wahl.



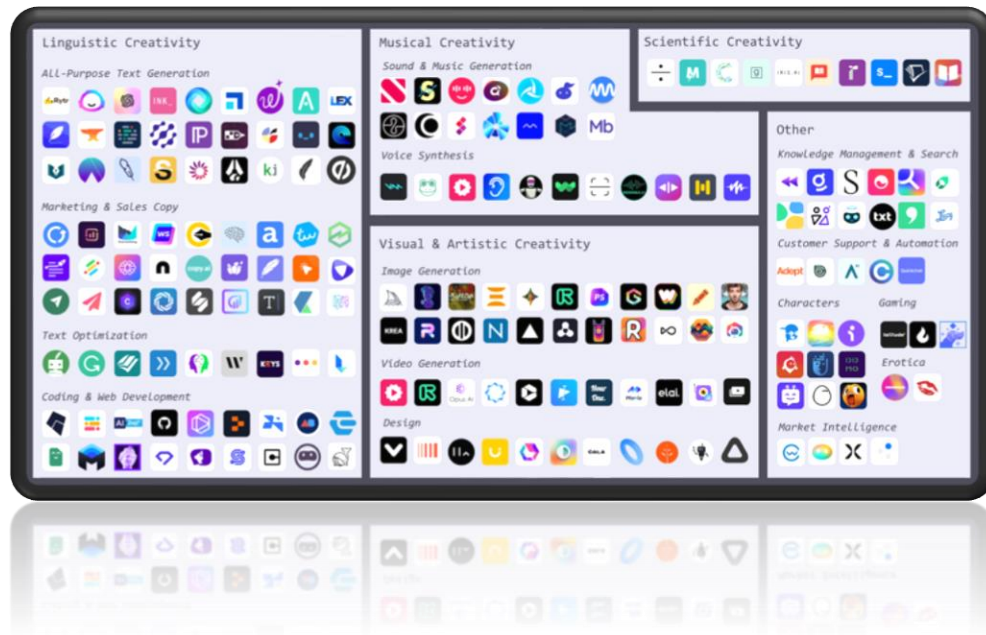
FUNCTIONAL ADD-ONS

- Managed XDR
- Intelligent Last-Mile Management

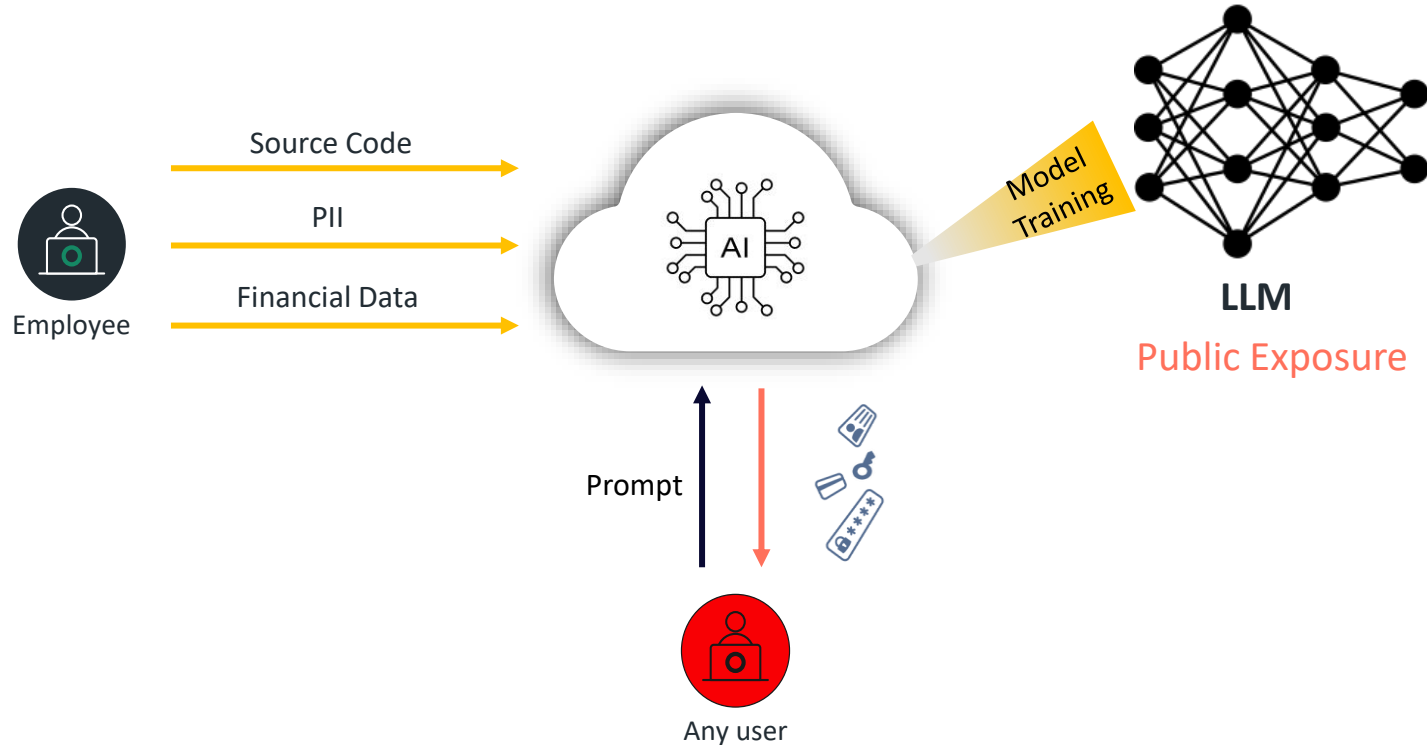
Erweitern Sie den
Funktionsumfang – so individuell,
wie Ihr Schutzbedarf.

Der generative KI-Wildwuchs

- **Welche** Anwendungen sind im Einsatz?
- **Wer** nutzt sie?
- **Wie** werden sie genutzt?
- **Wo** befinden sich meine sensiblen Daten?



Das Risiko: Herausgabe sensibler Informationen



Die Realität

AI/ML, Training, Data Security

38% of AI-using employees admit to sending sensitive work data

September 26, 2024



By Laura French



Adobe Stock

More than a third of employees who use AI for work admit to sending information to AI applications without their employer's knowledge, a Cybersecurity Alliance (NCA) and CybSafe found.



Nearly 10% of employee gen AI prompts include sensitive data

News Analysis

10 Feb 2025 • 6 mins

Data and Information Security

Generative AI

Enterprise users are leaking sensitive corporate data through use of unauthorized and authorized generative AI apps at alarming rates. Plugging the leaks is vital to reduce risk exposure.

12,000+ API Keys and Passwords Found in Public Datasets Used for LLM Training

Feb 28, 2025 • Ravie Lakshmanan

Machine Learning / Data Privacy



A dataset used to train large language models (LLMs) has been found to contain nearly 12,000 live secrets, which allow for successful authentication.

The findings once again highlight how hard-coded credentials pose a severe security risk to users and organizations alike, not to mention compounding the problem when LLMs end up suggesting insecure coding practices to their users.

The Hacker News



Trending News

GenAI Use Cases

SHADOW AI - VISIBILITY



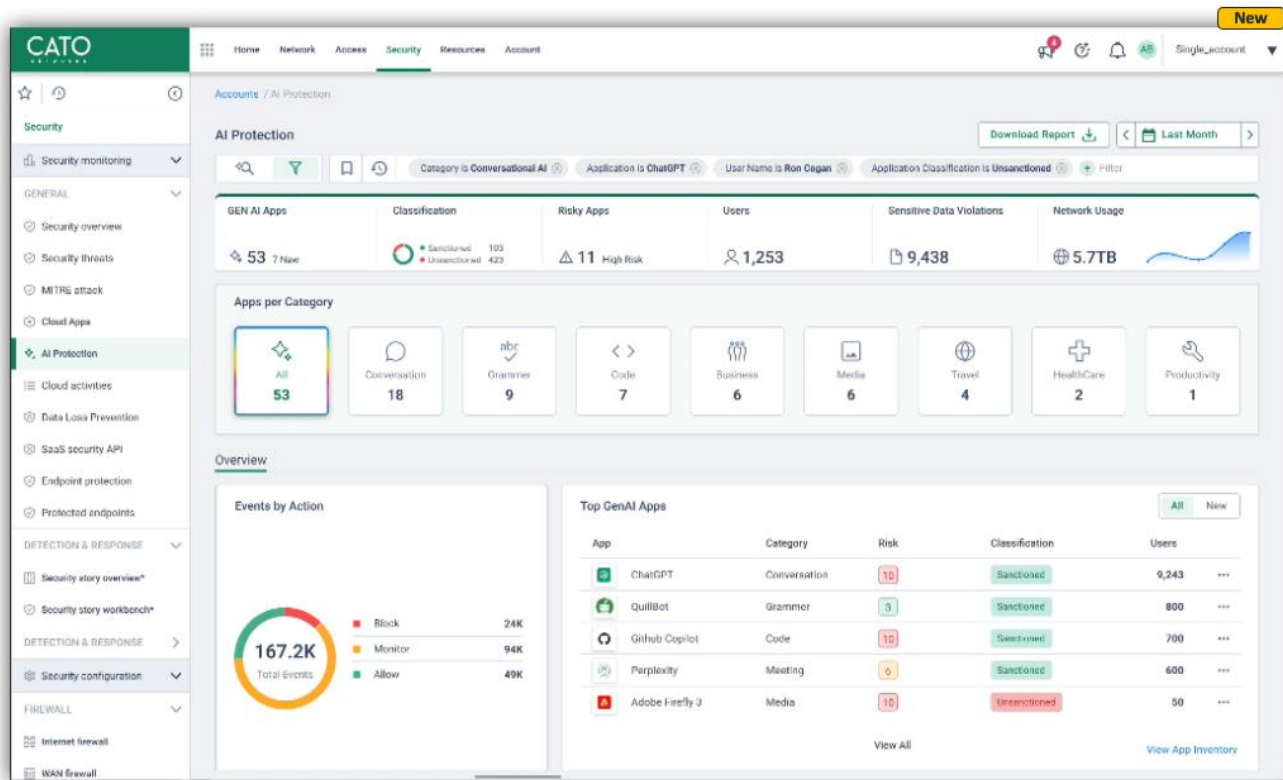
ACCESS CONTROL - SECURITY



DATA PROTECTION - SECURITY



AI Protection Dashboard



Human. Technology. Together.



Consulteer
InCyber