IT Security Architecture

-

Neue Ansätze und Lösungen

Manuel Götz

Consultant

CCNP Security

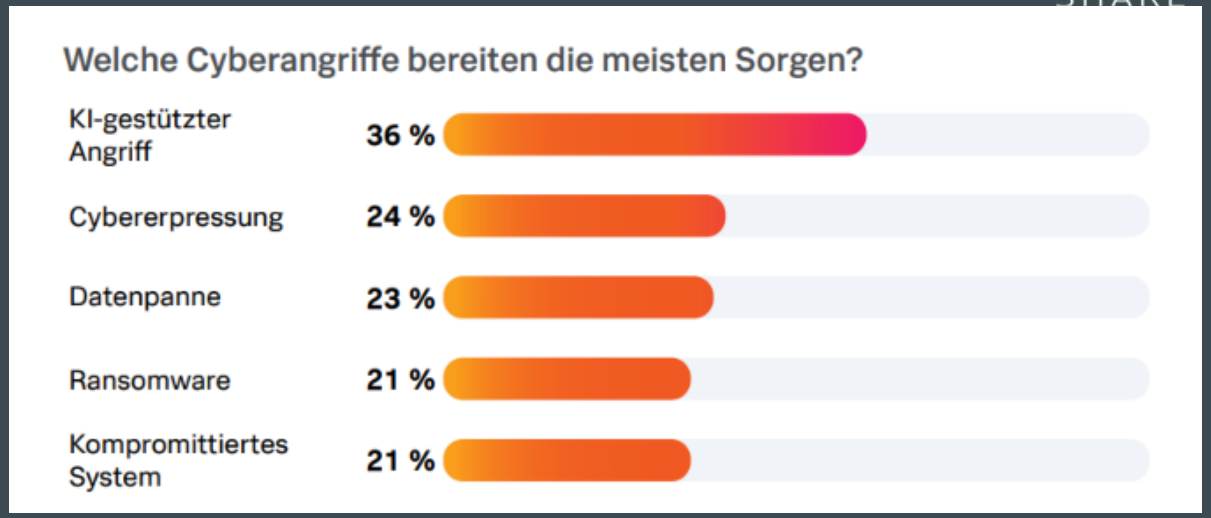
IT for innovators.

Alexander Knauff

Senior Support Engineer

IT for innovators.

Lagebericht Security 2024



Probleme in der IT Security

- Viele Hersteller
- Hohe Komplexität
- Versteckte Sicherheitslücken
- Entwicklungen finden sehr schnell statt
- Bedrohungslandschaft wächst

IT Security Architecture

Neue Ansätze und Lösungen

SASE

SSE

Global Access

Multicloud Defense

Secure Access

Cisco Security AI

ZTNA

Containerized Firewall

Microsoft Copilot

Hypershield

Secure Service Edge
SSE

„Ich brauche Security, die mit den neuesten Bedrohungen mithalten kann!“

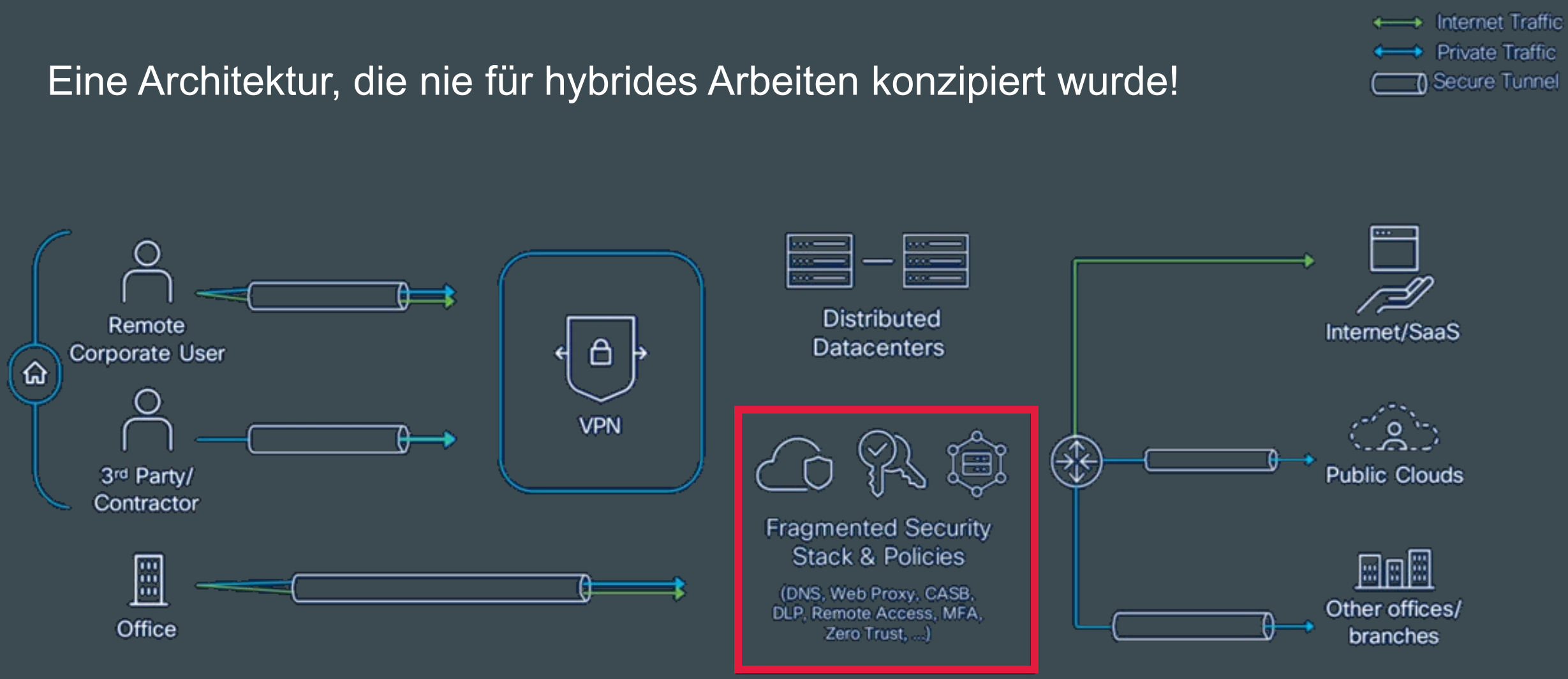
„Es gibt zu viele verschiedene Security Tools, sehe ich wirklich alles?“

„Die IT-Security steht der Produktivität der Mitarbeiter im Weg!“

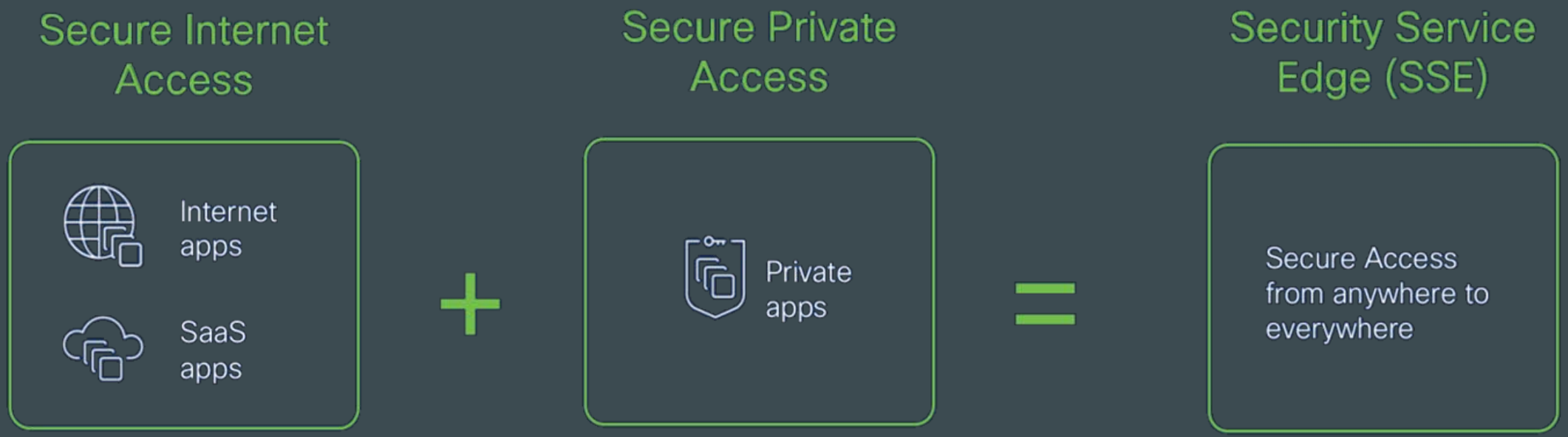
Homeoffice

Herausforderung

Eine Architektur, die nie für hybrides Arbeiten konzipiert wurde!



Use Cases unserer Kunden



Secure Service Edge
SSE

Dezentrale Security

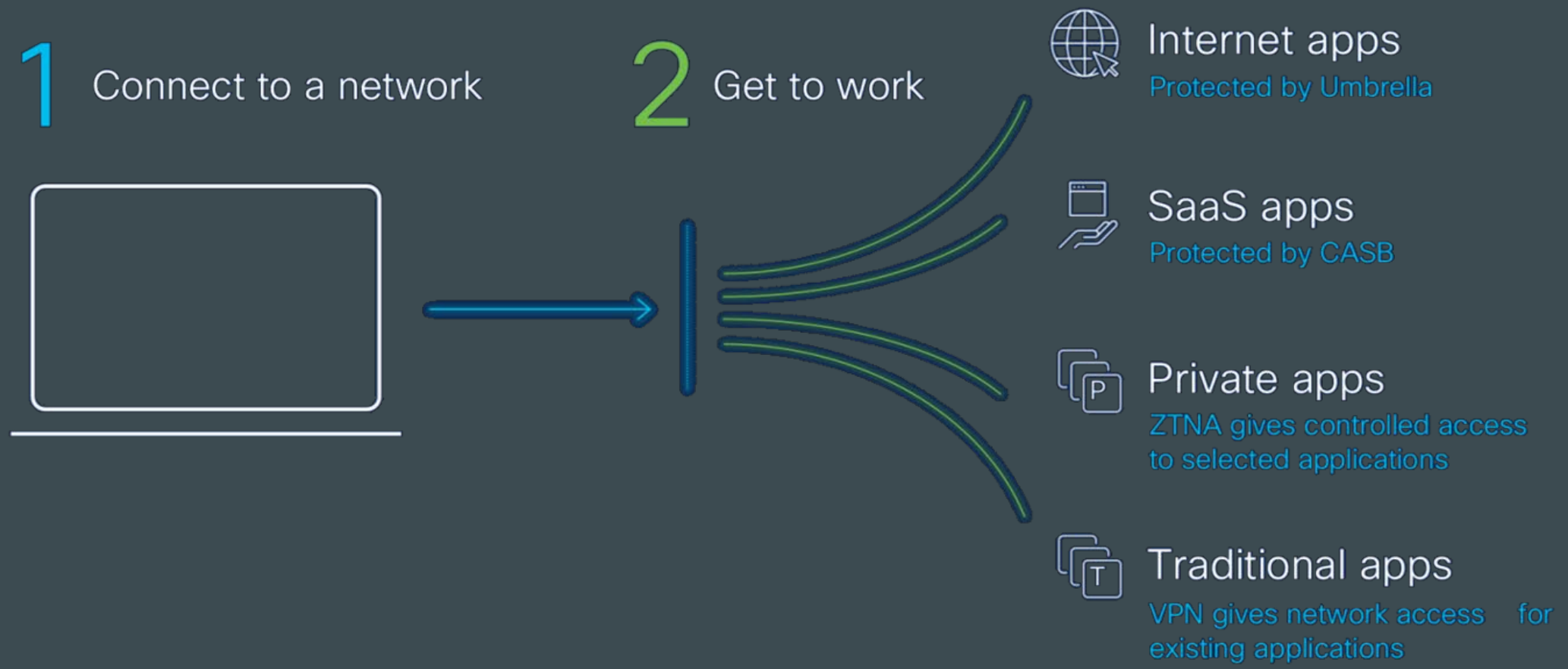
Zentrales Security-Management

Durchgängige Sicherheitsrichtlinie

Ein Dashboard

Modular erweiterbar

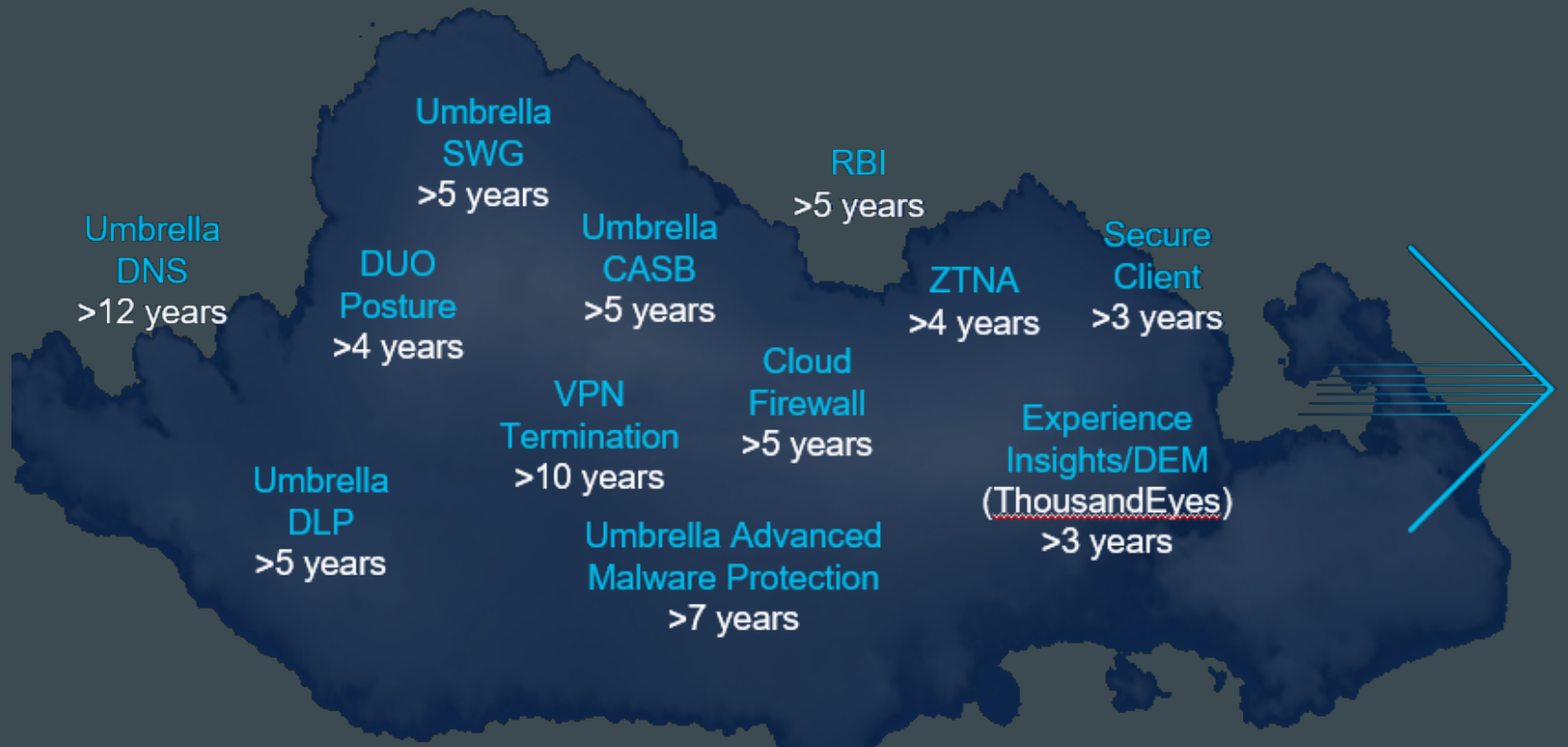
Cloudbasiert


1 Connect to a network
2 Get to work
Internet apps
Protected by Umbrella
SaaS apps
Protected by CASB
Private apps
ZTNA gives controlled access to selected applications
Traditional apps
VPN gives network access for existing applications

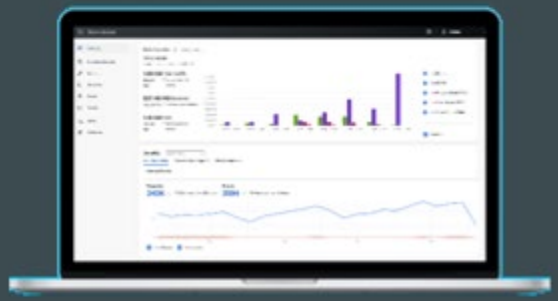
Cisco Secure Access

Introducing Cisco Secure Access

Proven cloud-native security converged into one service



Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

Protecting 70,000+ customers | More than 220M endpoints

Cisco Secure Access

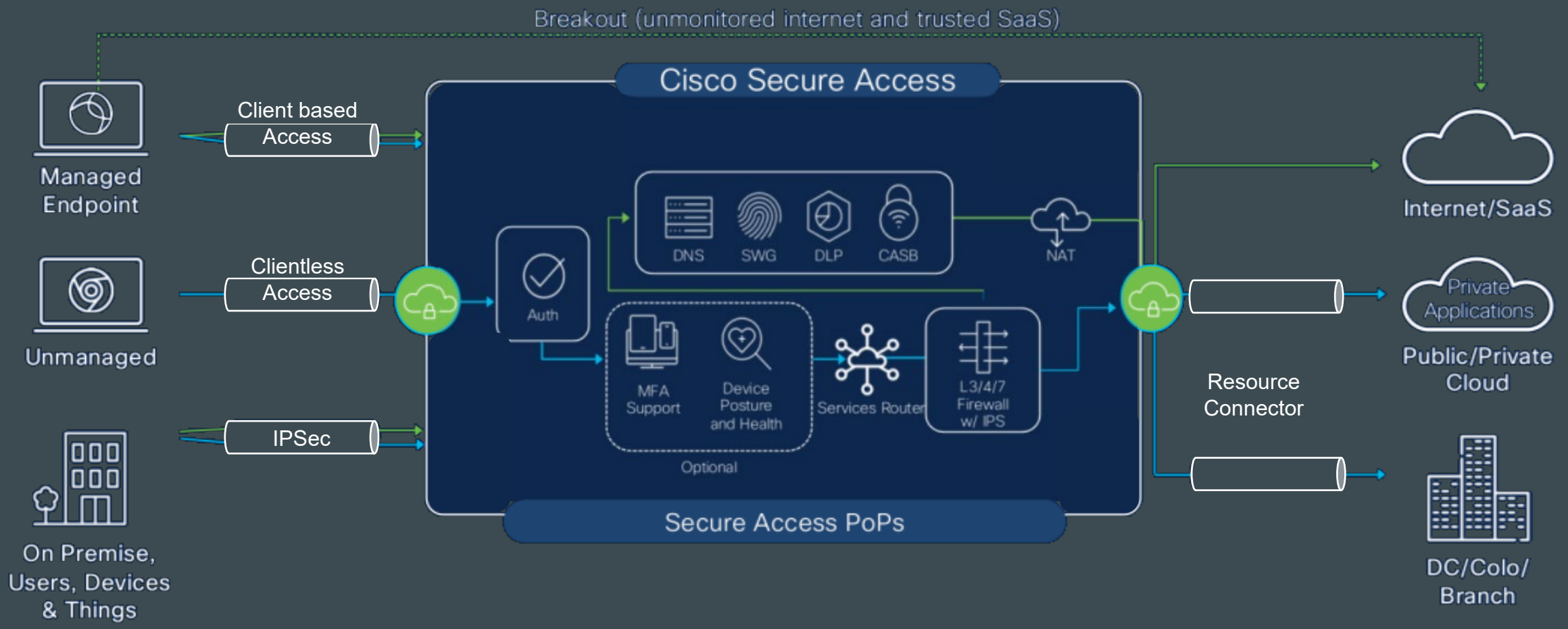
Core Capabilities

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) & DLP
- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS) & IPS

Beyond Core Capabilities

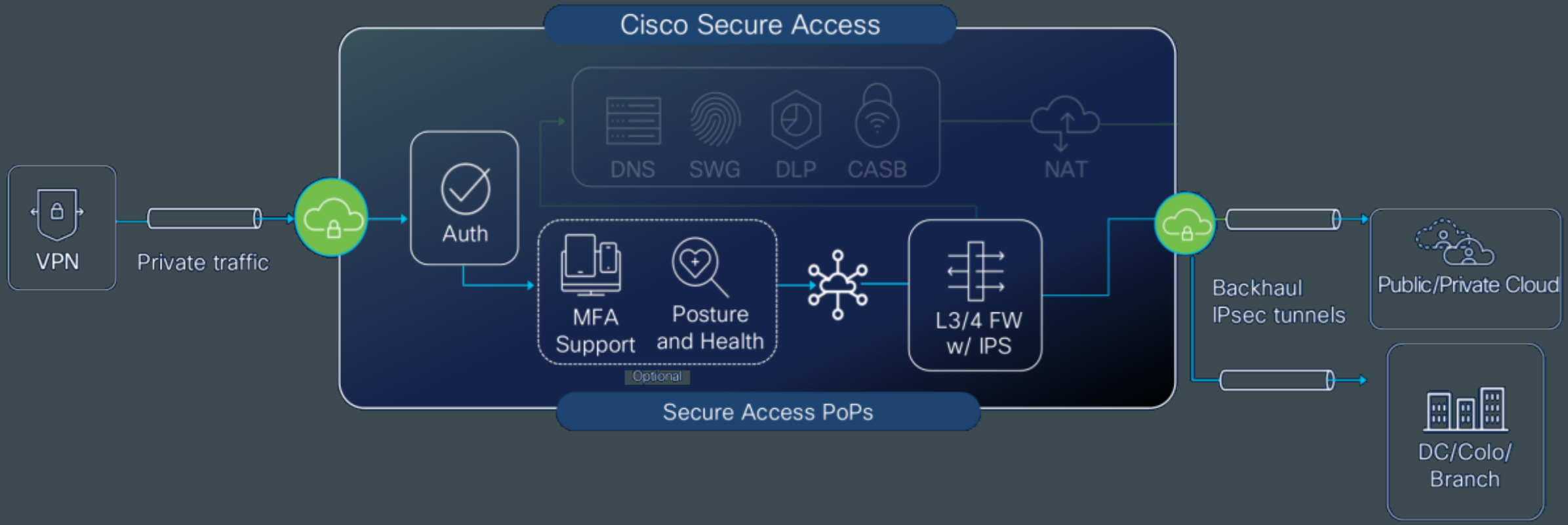
- DNS Security
- Multimode DLP
- Remote Browser Isolation
- Advanced Malware Protection
- File Sandbox
- TALOS
- VPN as a Service
- AI Assistant
- ISE Integration
- Apple Private Relay
- Digital Experience Monitoring (DEM) (ThousandEyes)
- SD-WAN Integration

Architecture Overview



Users — How — Apps

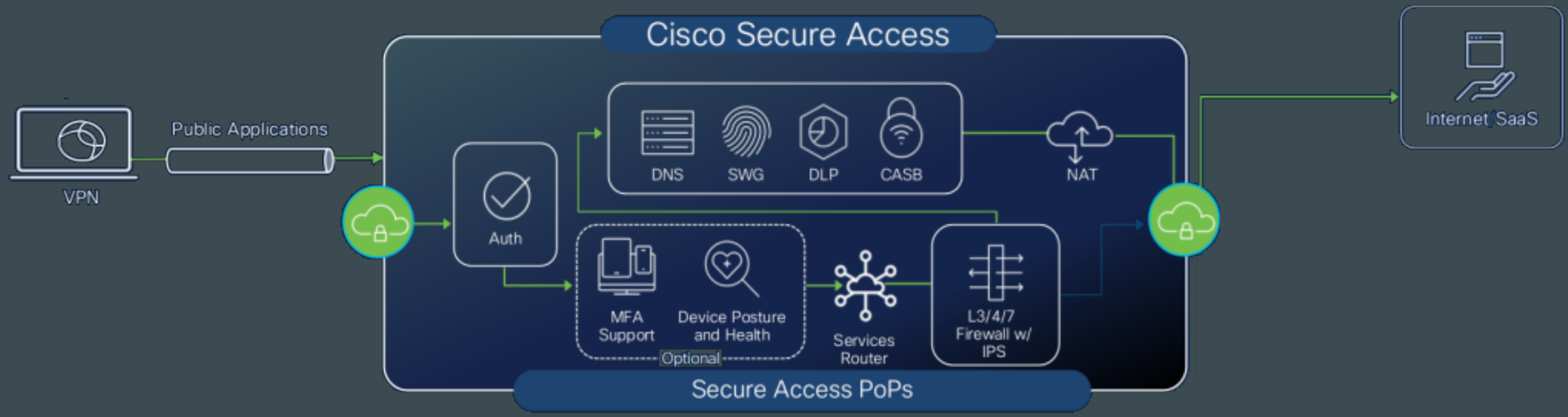
Secure Private Access



Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

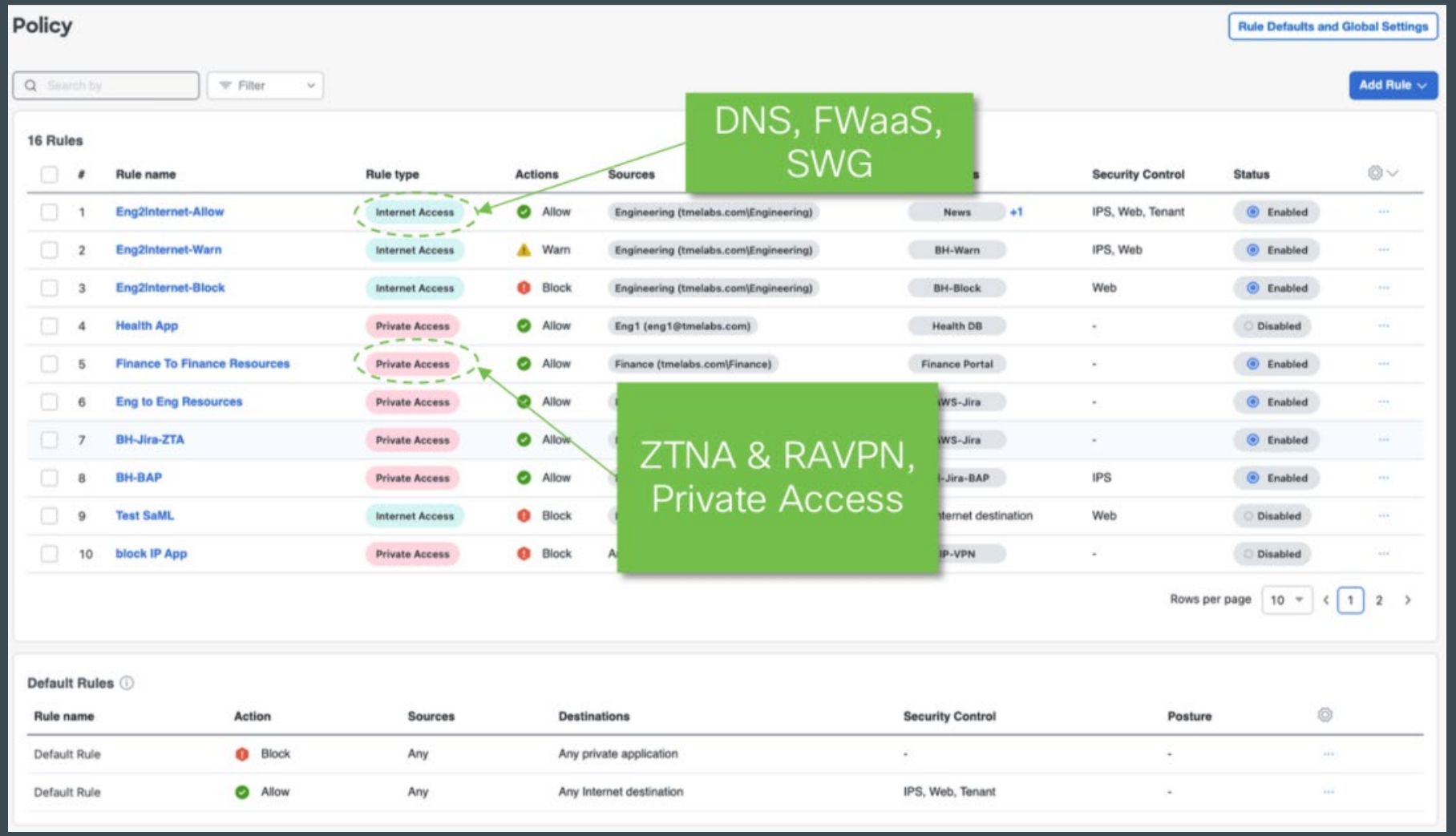
Secure Internet Access



Capabilities

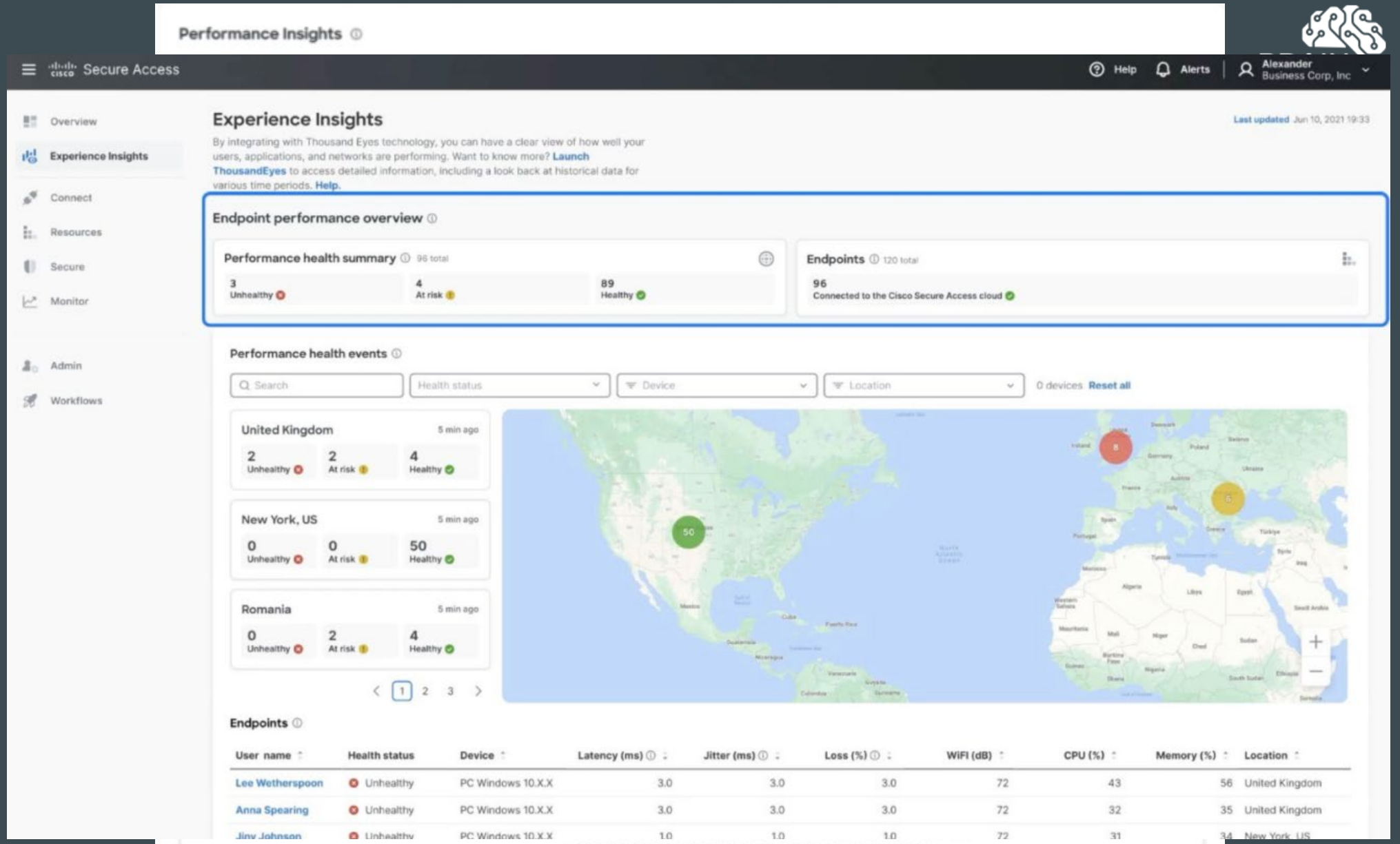
- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- IPS
- Single Inline inspection
- Application policy

Unified Policy!



Digital Experience Monitoring

Identifizierung und Lösung von Problemen



Top 20 SaaS Application Health

Common SaaS applications Performance

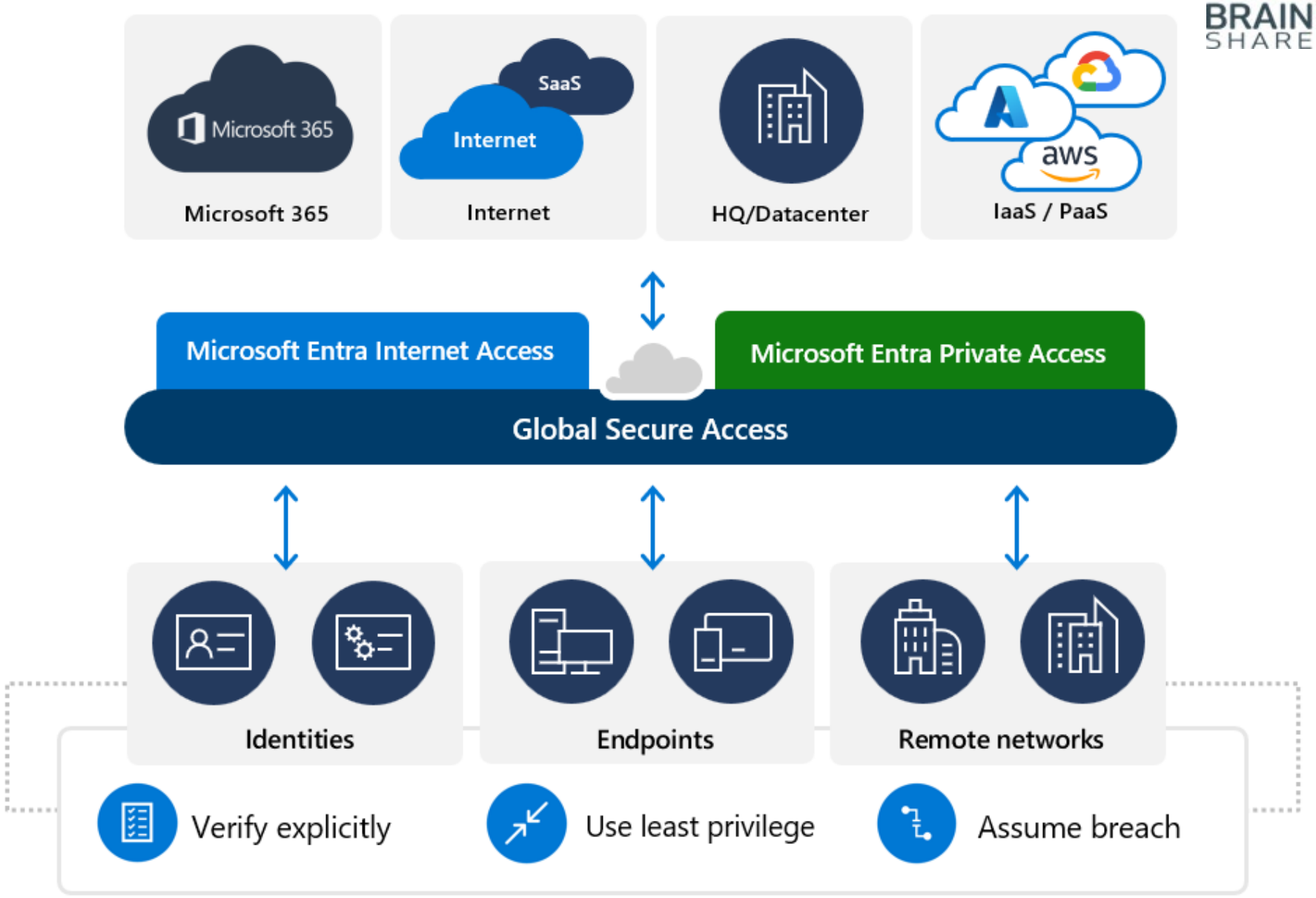
Search | US (Pacific Northwest) | Status | 20 applications

Status	Application	URL (Domain)	Response Time	Response Code	Description
✓	AWS	aws.amazon.com	76 ms	200	OK
✓	Bing	www.bing.com	58 ms	200	OK
✓	Box	www.box.com	117 ms	200	OK
✓	Confluence	confluence.atlassian.com	60 ms	200	OK
✓	DocuSign	www.docusign.com	262 ms	200	OK
✓	Dropbox	www.dropbox.com	978 ms	200	OK
✓	Figma	www.figma.com	55 ms	200	OK
✓	Gmail	mail.google.com	98 ms	200	OK
✓	Google Docs	docs.google.com	101 ms	200	OK
✓	Google Drive	drive.google.com	109 ms	200	OK
✓	Google Workspace	workspace.google.com	44 ms	200	OK
✓	Jira	jira.atlassian.com	15 ms	200	OK
✓	Microsoft 365	www.office.com	88 ms	200	OK
✓	Monday.com	monday.com	660 ms	200	OK
✓	Outlook	outlook.office.com	342 ms	200	OK
✓	Salesforce	www.salesforce.com	162 ms	200	OK


Microsoft Global Secure Access

Global Secure Access

Technischer Überblick

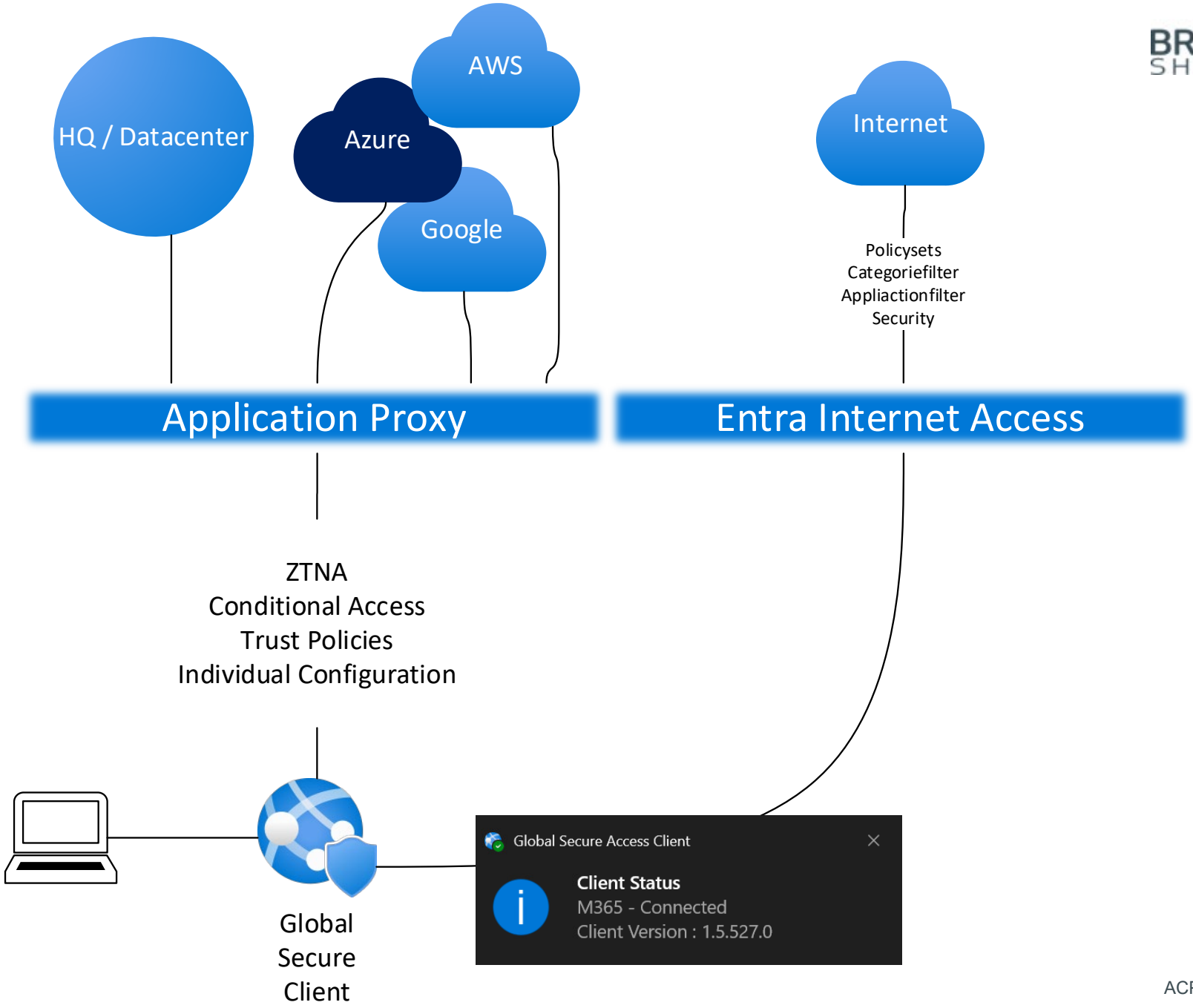


Quellen: https://www.microsoft.com/

Global Secure Access

Global Secure Access Client

Firmennetz
jederzeit und überall

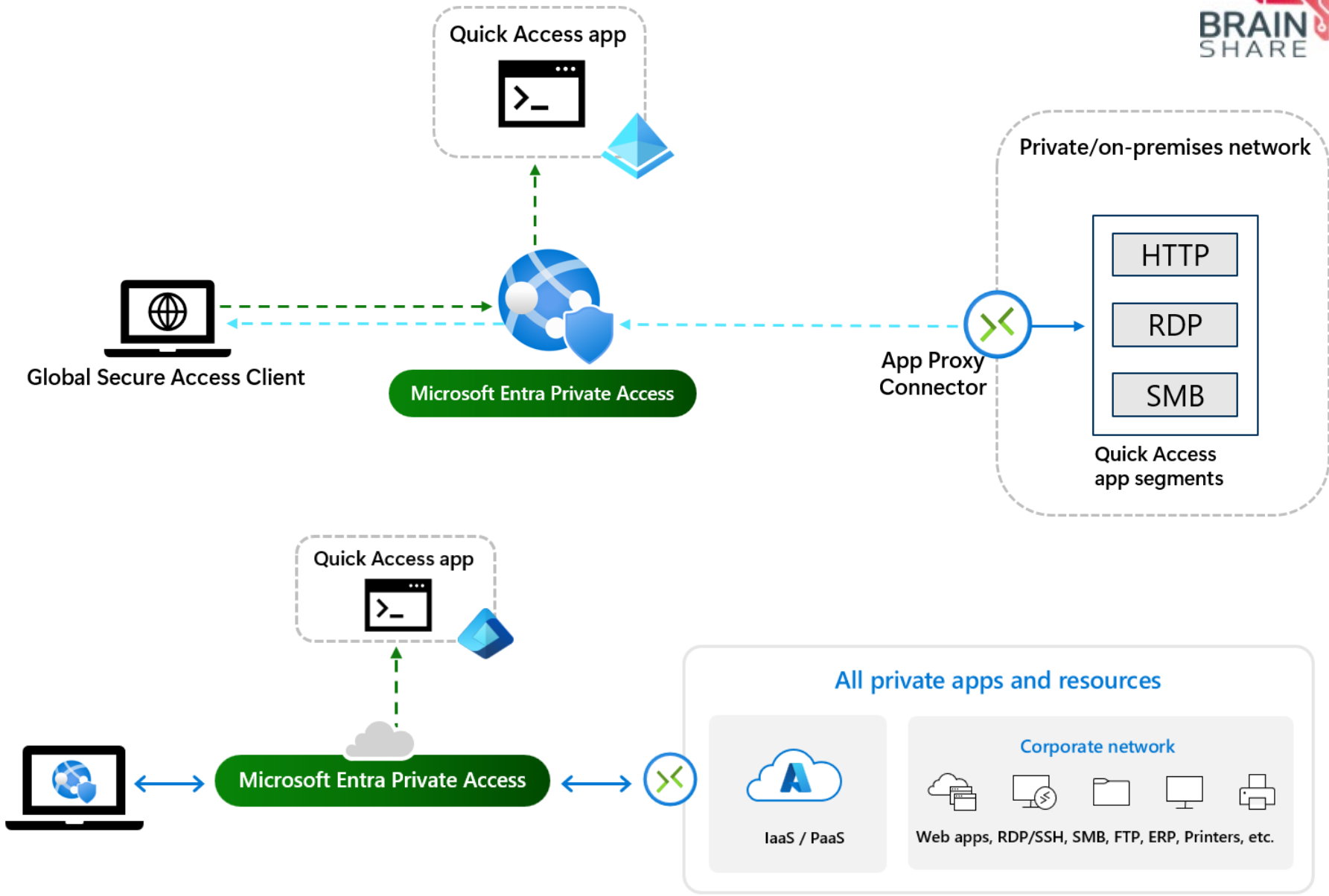


Quellen: https://www.microsoft.com/

Global Secure Access

Firmennetz

Zugriff von extern

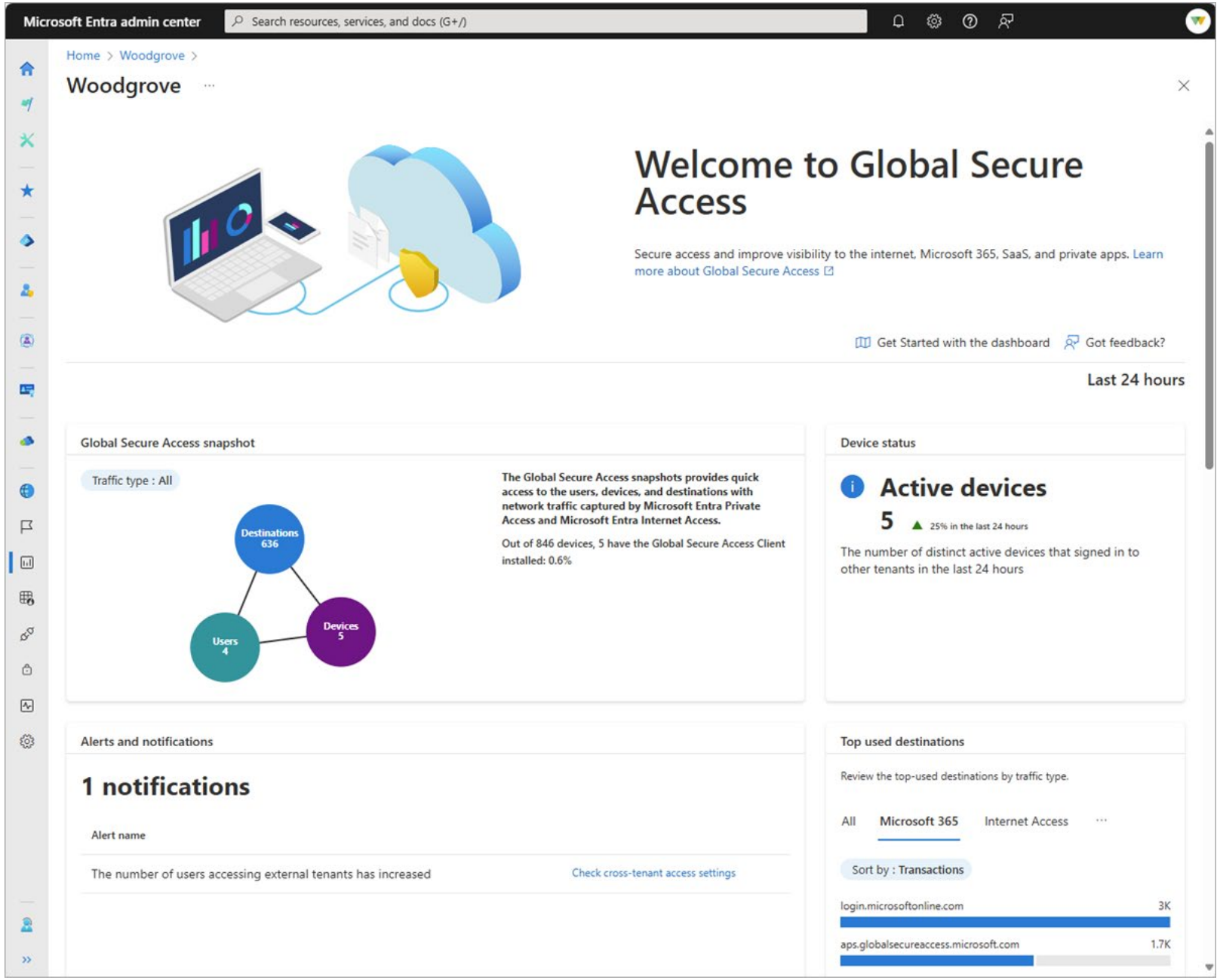


Quellen: https://www.microsoft.com/

Global Secure Access

Ein Dashboard

Alle Daten in
einer Plattform



Quellen: https://www.microsoft.com/

Secure Service Edge (SSE)

- Sicherheit zentral steuern
- Schnelle Reaktion auf Events
- Zugang an einer Stelle regeln
- Nutzerzufriedenheit steigern

Künstliche Intelligenz und Cybersecurity

„Langfristig werden sich KI-Modelle in ihrer Fähigkeit und Leistung kontinuierlich verbessern und weiterentwickeln. Daher könnte KI im Bereich Cybercrime als Katalysator wirken und einen enormen Anstieg der Kriminalität auslösen.“

(Cybercrime: Bundeslagebild 2023 vom Bundeskriminalamt)

Die Cyberbedrohungslandschaft verändert sich für Angreifer und Verteidiger

Social Engineering Angriffe

z.B. Deepfakes oder personalisiertes Phishing

Technische Angriffsvektoren

z.B. KI gestützte Anwendungen, Hacker-KI

IT for innovators.

ACP

BRAIN SHARE

Einfluss von KI auf die Cyberbedrohungslandschaft

10.04.2024

Bundesamt
für Sicherheit in der
Informationstechnik

IT for innovators.

1 Einleitung

Mit dem Aufkommen von Anwendungen, die auf großen Sprachmodellen (eng. „large language models", LLM) basieren, ist KI auch in der Öffentlichkeit wieder ein viel diskutiertes Thema. Die Grenzen dieser neuen Modelle müssen noch erforscht werden und es ist unklar, welche bleibenden Veränderungen der aktuelle KI-Trend mit sich bringt. Zweifelsohne gibt es Bedenken hinsichtlich der Auswirkungen von KI auf die Cybersicherheit, da sie bereits jetzt die Cyberbedrohungslandschaft sowohl für Angreifer als auch für Verteidiger verändert. Wir untersuchen, wie sich Angriffe und Tätigkeiten von Angreifern durch die neu verfügbare Technologie verändern, wobei wir uns auf die offensive Nutzung von KI konzentrieren. Während generative KI bereits die Qualität und Quantität von Social-Engineering-Angriffen steigert (z. B. Deepfakes oder personalisiertes Phishing in großem Maße), fokussieren wir unsere Diskussion mehr auf technische Angriffsvektoren und weniger auf den menschlichen Faktor. Es sollte jedoch erwähnt werden, dass Social-Engineering-Angriffe zu den häufigsten Angriffen gehören und KI auf diese Art von Angriff starke Auswirkungen hat.

Konkret geht es uns nicht darum, alle Möglichkeiten in diesem weiten Feld zu erörtern. Ziel dieses Berichts ist es, KI-gestützte Anwendungen zu identifizieren, die bereits für den offensiven Einsatz verfügbar sind und zu bewerten, wie sich diese Bedrohungen in naher Zukunft entwickeln könnten. Dazu gehören auch Tools und Anwendungen mit doppeltem Verwendungszweck (sog. Dual-Use-Güter), wie z. B. Penetrationstests, die sowohl beim ethischen Red-Teaming als auch bei kriminellen Aktivitäten helfen können. Wir befassen uns

ACP

BRAIN SHARE

Bundesamt für Sicherheit in der Informationstechnik

Einfluss von KI auf die Cyberbedrohungslandschaft

10.04.2024

Auswirkungen

- Überzeugende Phishing-Nachrichten
- Deepfakes
- Malware kann verschleiert werden
- Malware in KI-Systemen versteckt
- Erraten von Passwörtern
- Umgehen von Captchas

IT for innovators.

Das Gleichgewicht der Kräfte verschiebt sich, wenn eine Partei auf die Nutzung eines Vorteils verzichtet.

Cybersecurity

KI zur Verbesserung und Beschleunigung von

- Erkennung von Angriffen
- Durchführung von Gegenmaßnahmen
- Bewertung von Präventionsmaßnahmen
- Auswertung der Sicherheitslage

Entlastung der Administratoren

Vermeidung von Fehlern

IT for innovators.

Security AI

ASSIST

-

AUGMENT

-

AUTOMATE

ASSIST

AI Assistenten, die die Art und Weise, wie wir Menschen und Maschinen miteinander interagieren, erweitern

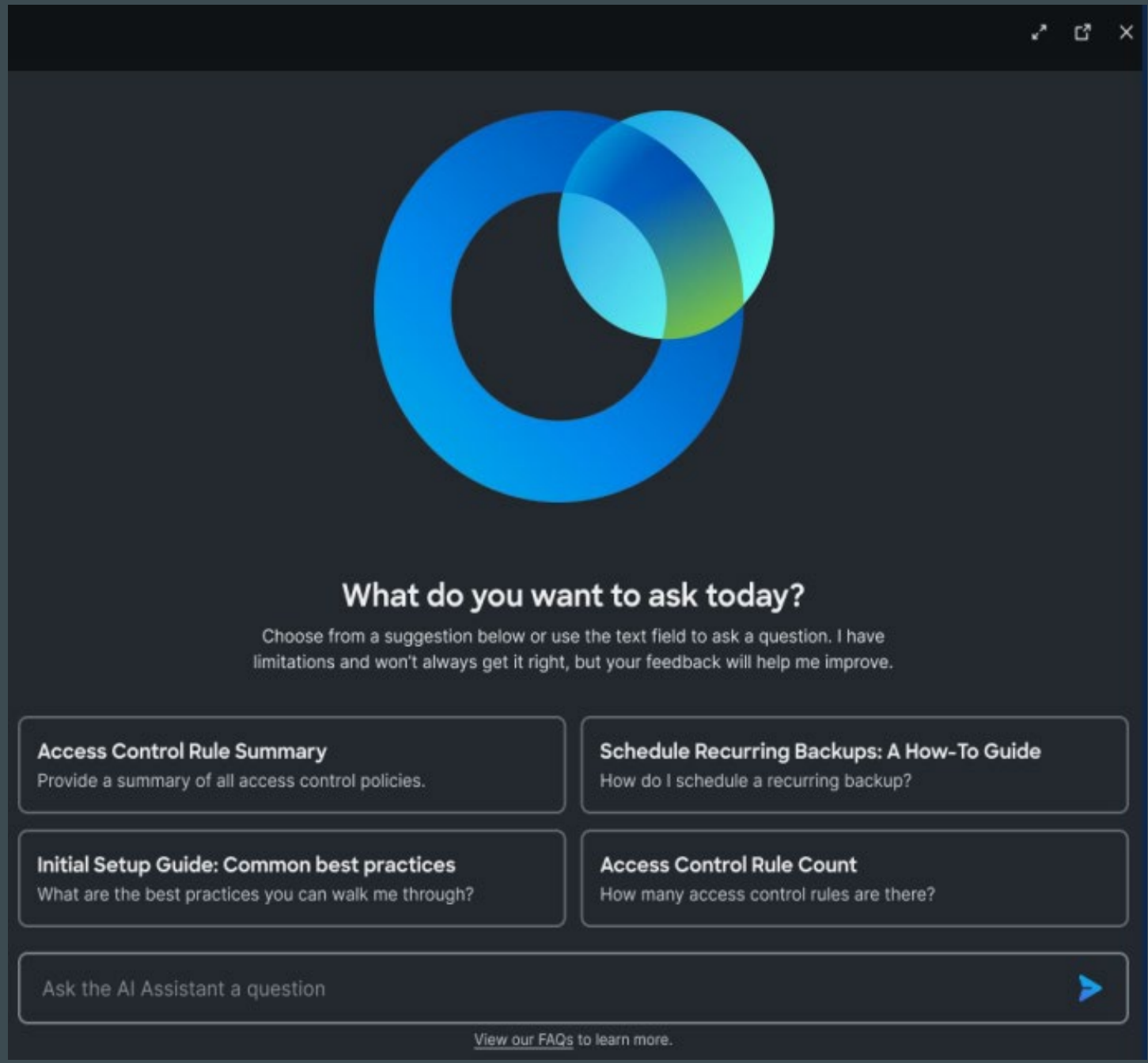

Cisco Security AI
CISCO
TM

AI Assistant in der Firewall

- Troubleshooting beschleunigen
- Schneller agieren
- Visibilität erhöhen
- Best Practises umsetzen

IT for innovators.

AI Assistant in der Secure Firewall



IT for innovators.

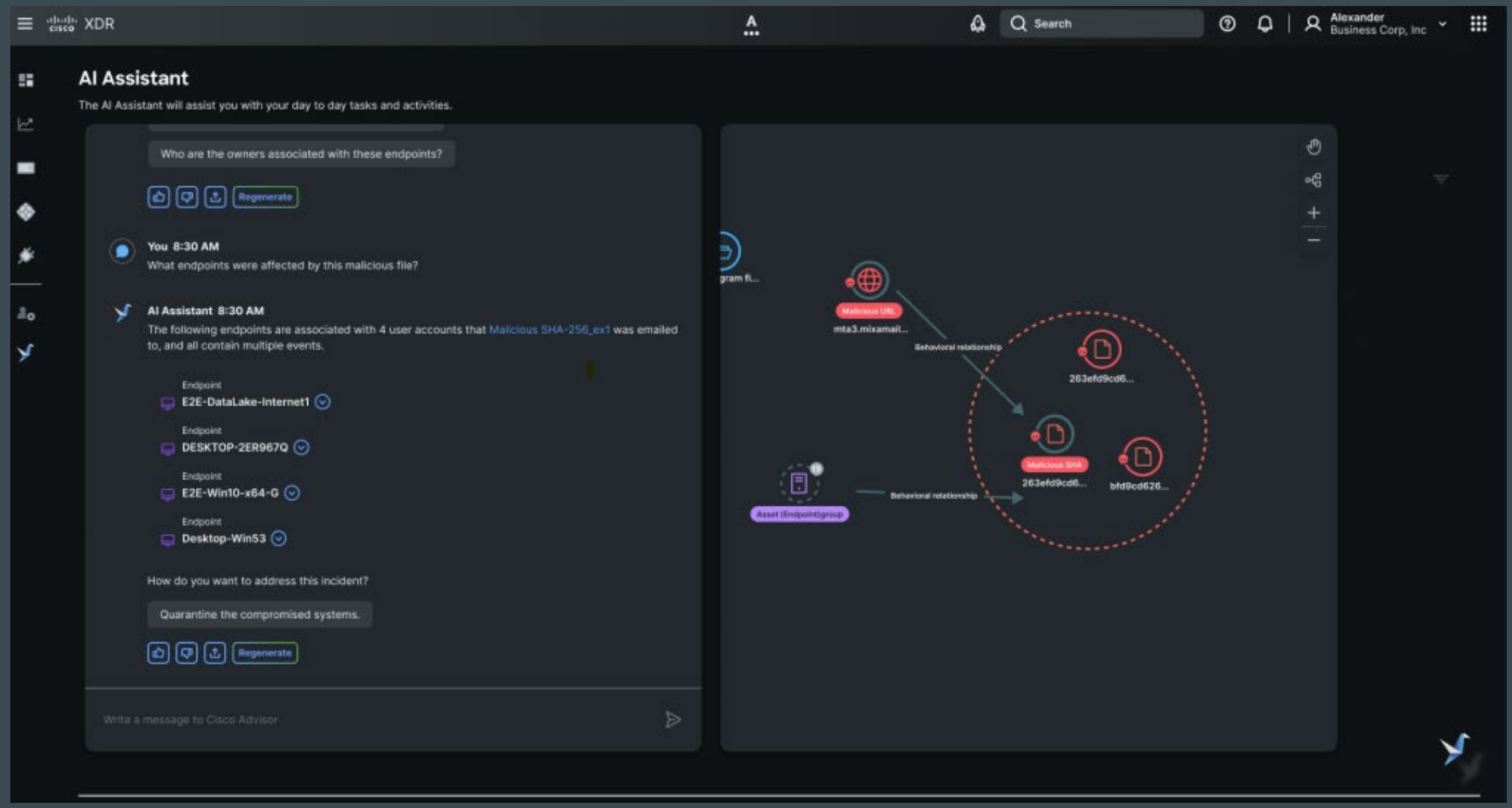
AI Assistant in XDR

- IOC´s untersuchen und nachverfolgen
- Incident Summaries
- Handlungsempfehlungen

IT for innovators.

XDR erkennt eine Phishing Attacke, die über C&C Daten abfließen lässt

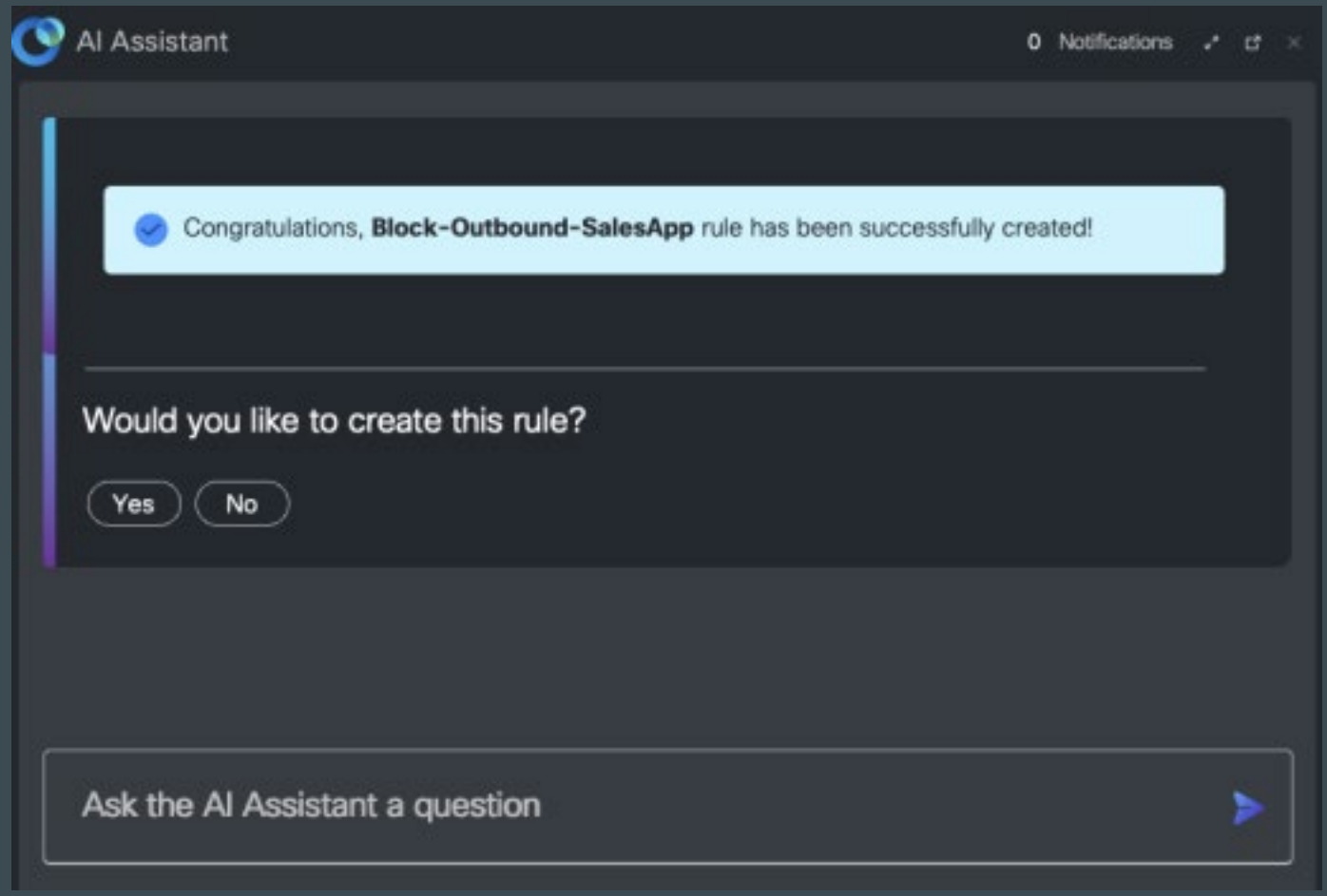
AI Assistant in XDR



IT for innovators.

AI Assistant in XDR

- Direkte Weiterleitung zum CDO mit allen Angriffsinformationen

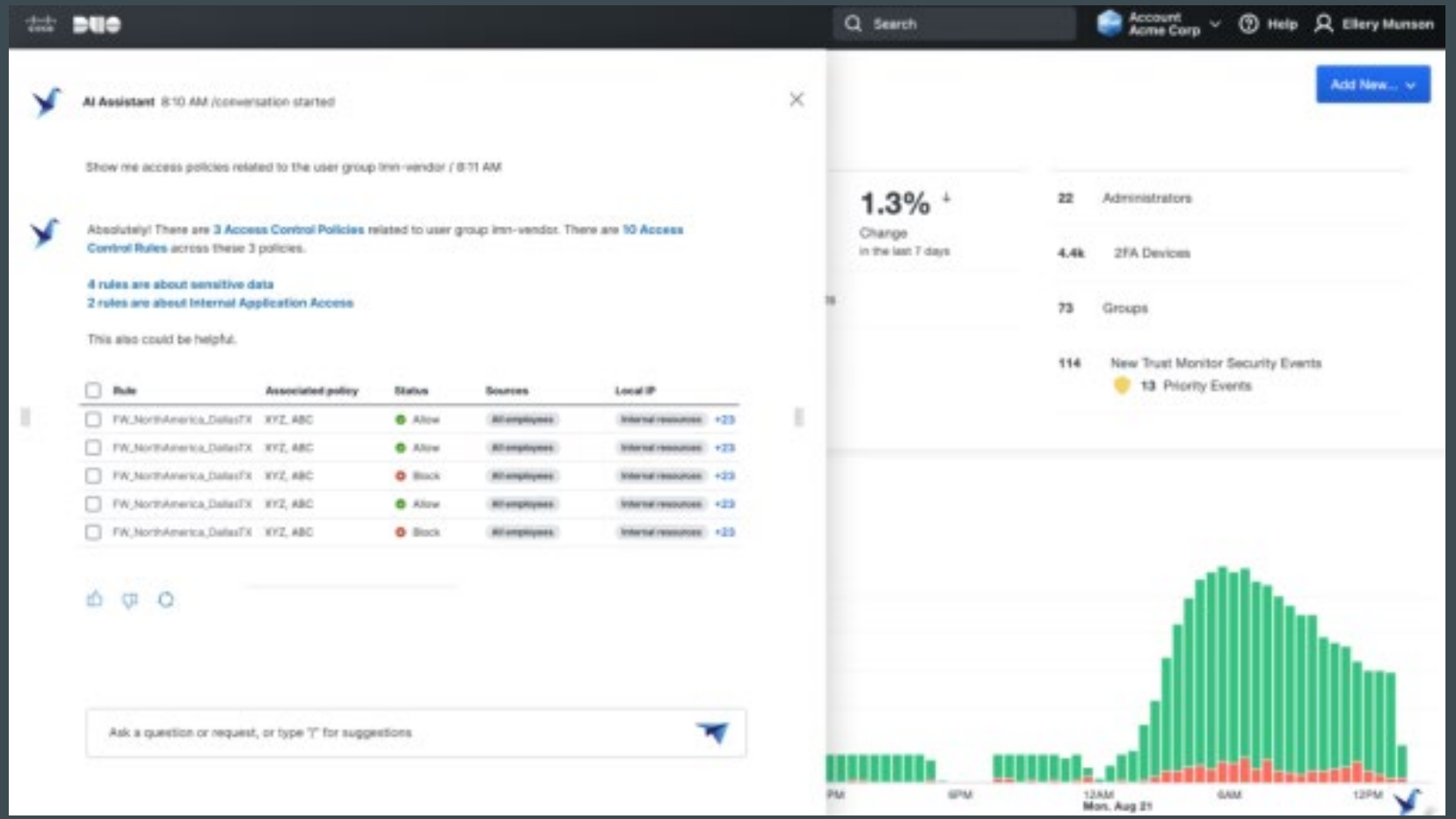


- Blockregel wird vorgeschlagen und kann direkt erstellt werden

IT for innovators.

AI Assistant in XDR

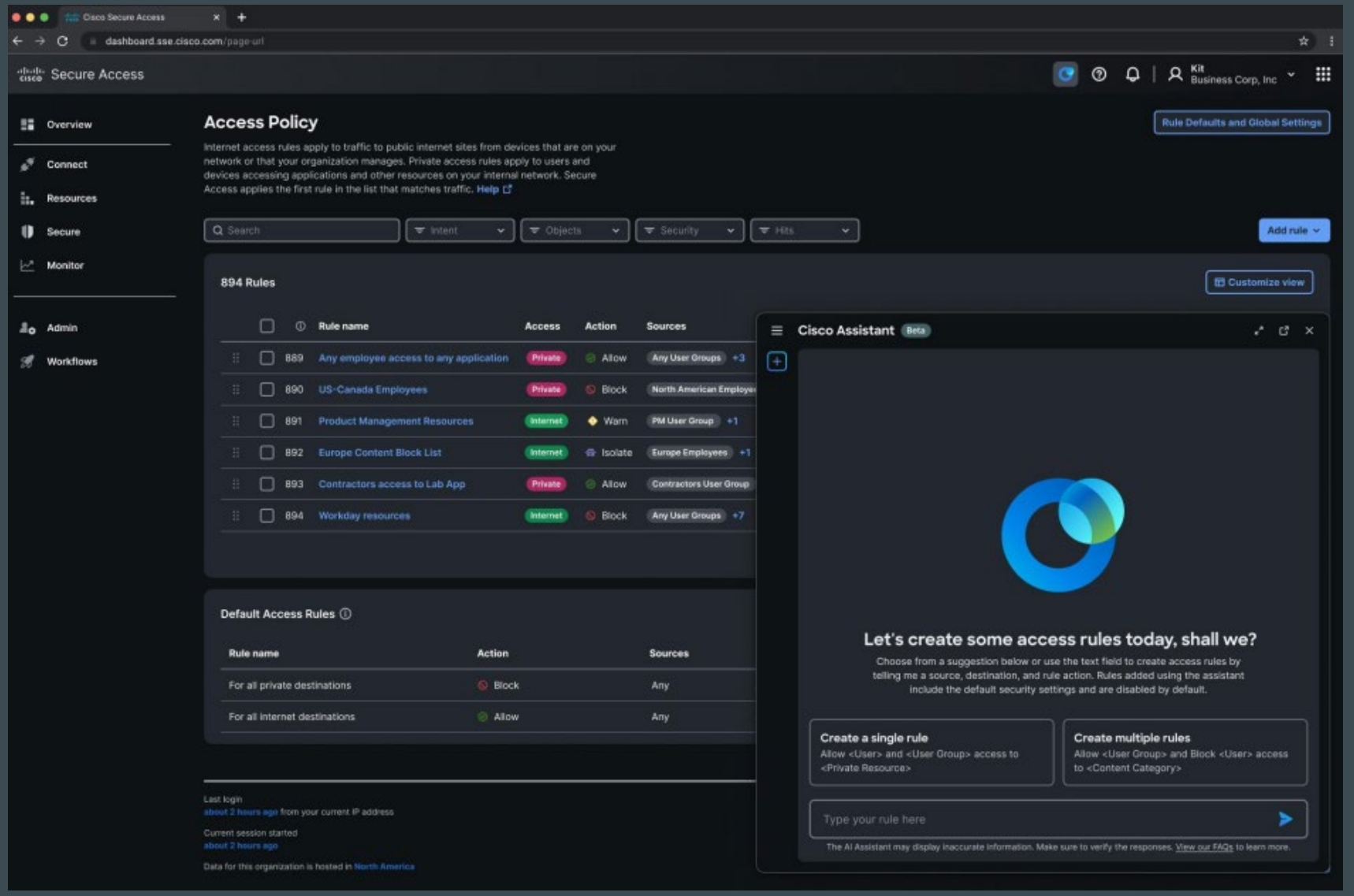
Mit einem weiteren Klick in der DUO Konsole den User von allen kritischen Applikationen aussperren



IT for innovators.

Policy administration beschleunigen

AI Assistant in Secure Access

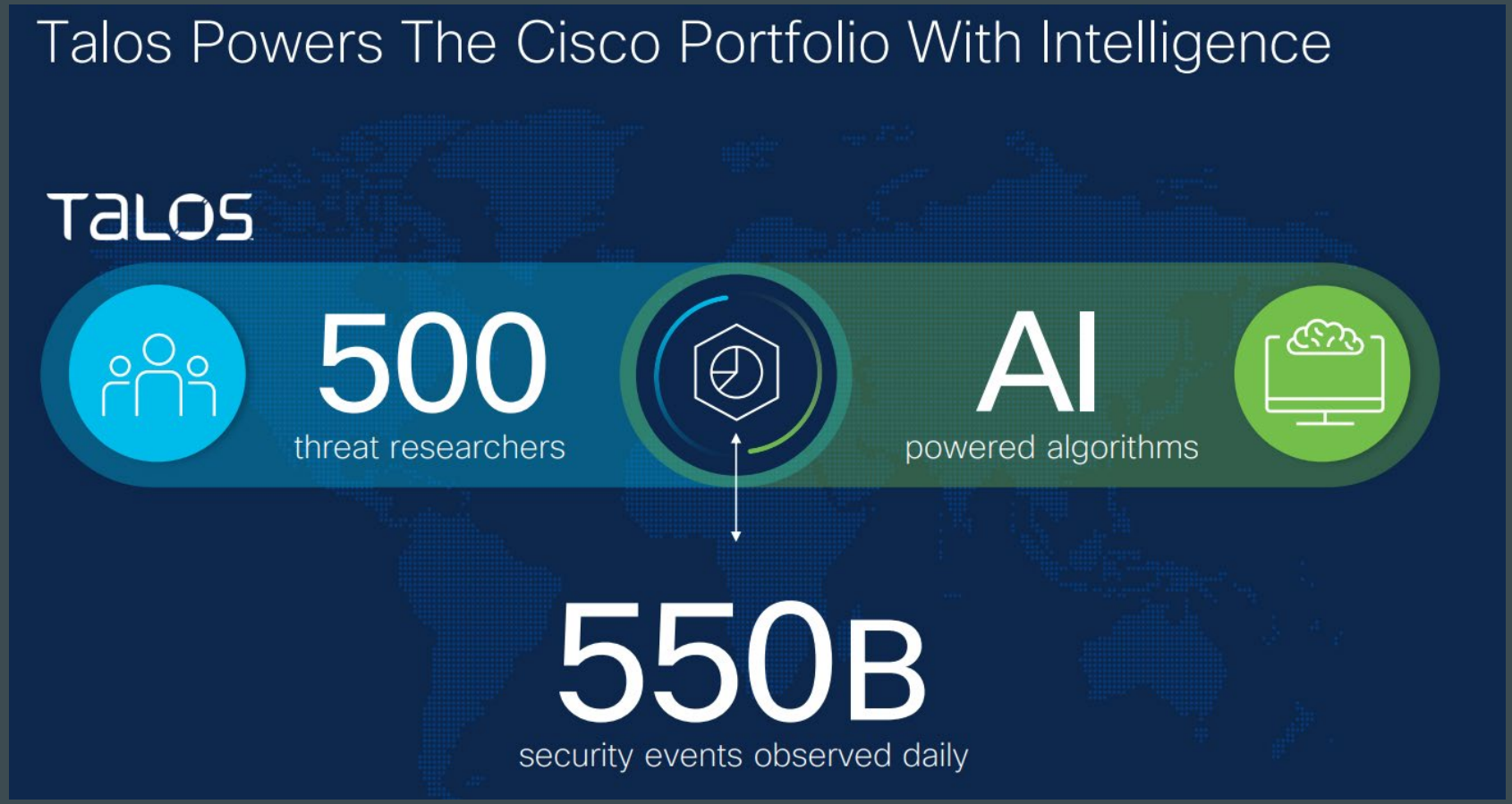


IT for innovators.


ACP
AUGMENT
Korrelierung und Überwachung
von Informationen und Events
mit maschineller
Geschwindigkeit

AI Powered Detection

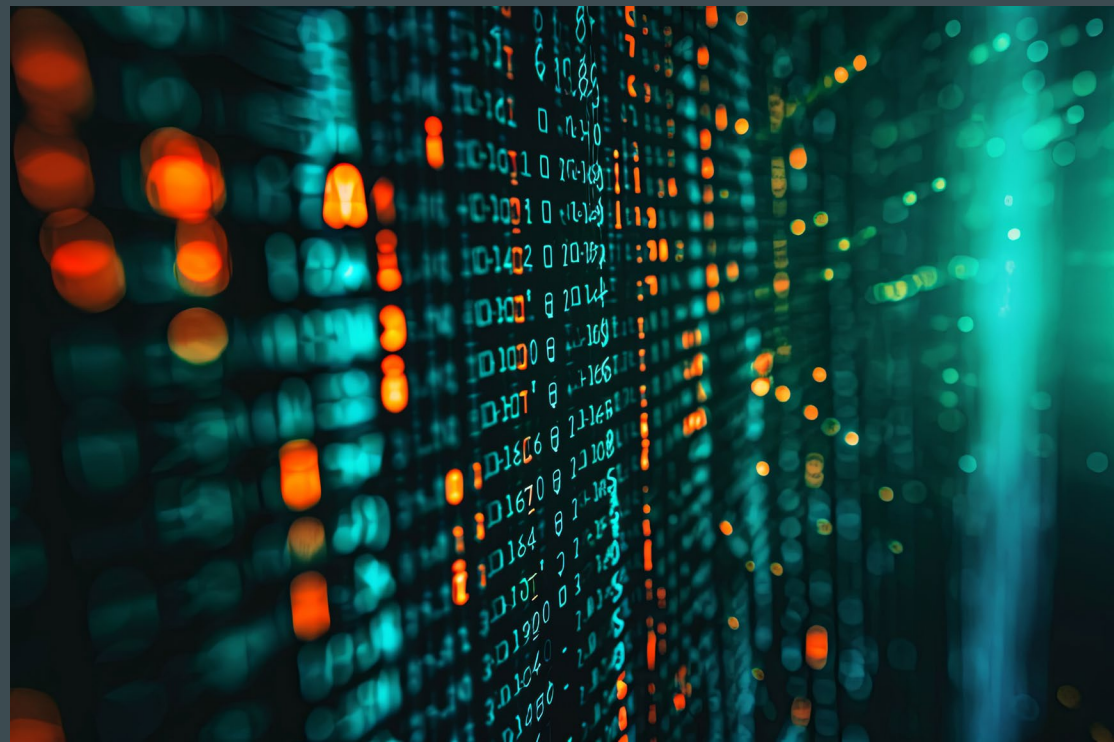
Korrelation von 555 Milliarden Security Events pro Tag



IT for innovators.

Ecrypted Visibility Engines (EVE)

- TLS verschlüsselter Traffic kann untersucht werden
- Fingerprints erkennen
- mit AI und ML Bedrohungen auswerten



IT for innovators.

AUTOMATE

Automatisierung komplexer Arbeitsabläufe die IT-Administratoren in jeglicher Hinsicht unterstützen

Autonomous Actions

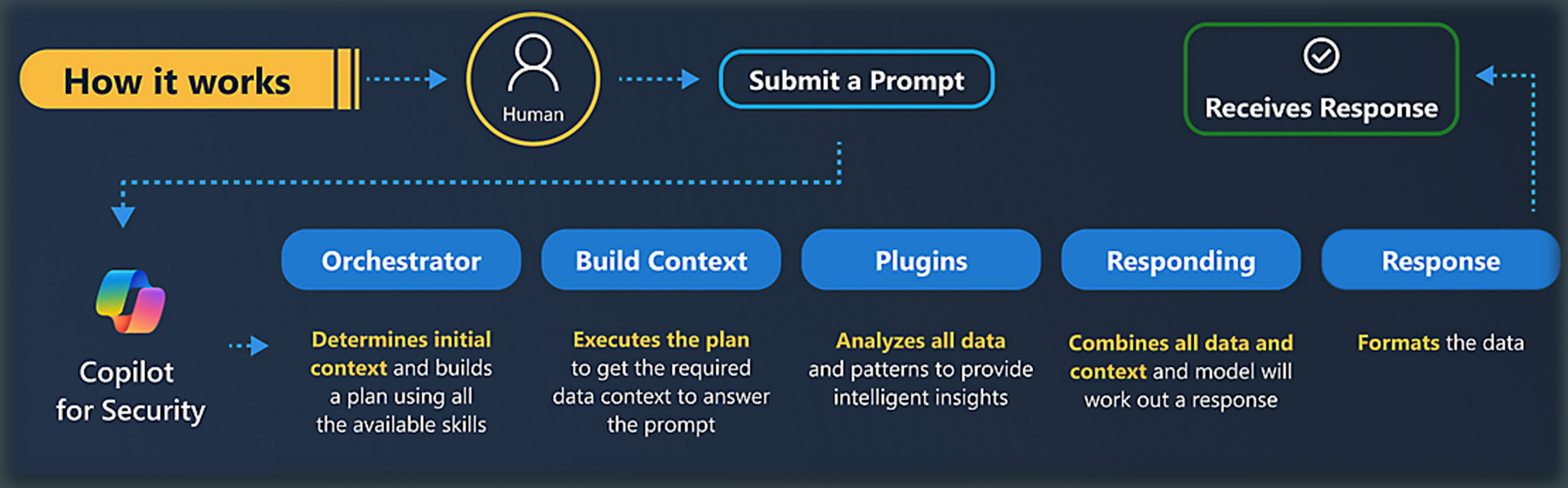
Aus Mensch-zu-Maschine Interaktionen lernen, um komplexe Playbooks zu erstellen

IT for innovators.

Copilot für Security

Quellen: https://www.microsoft.com/

Copilot für Security

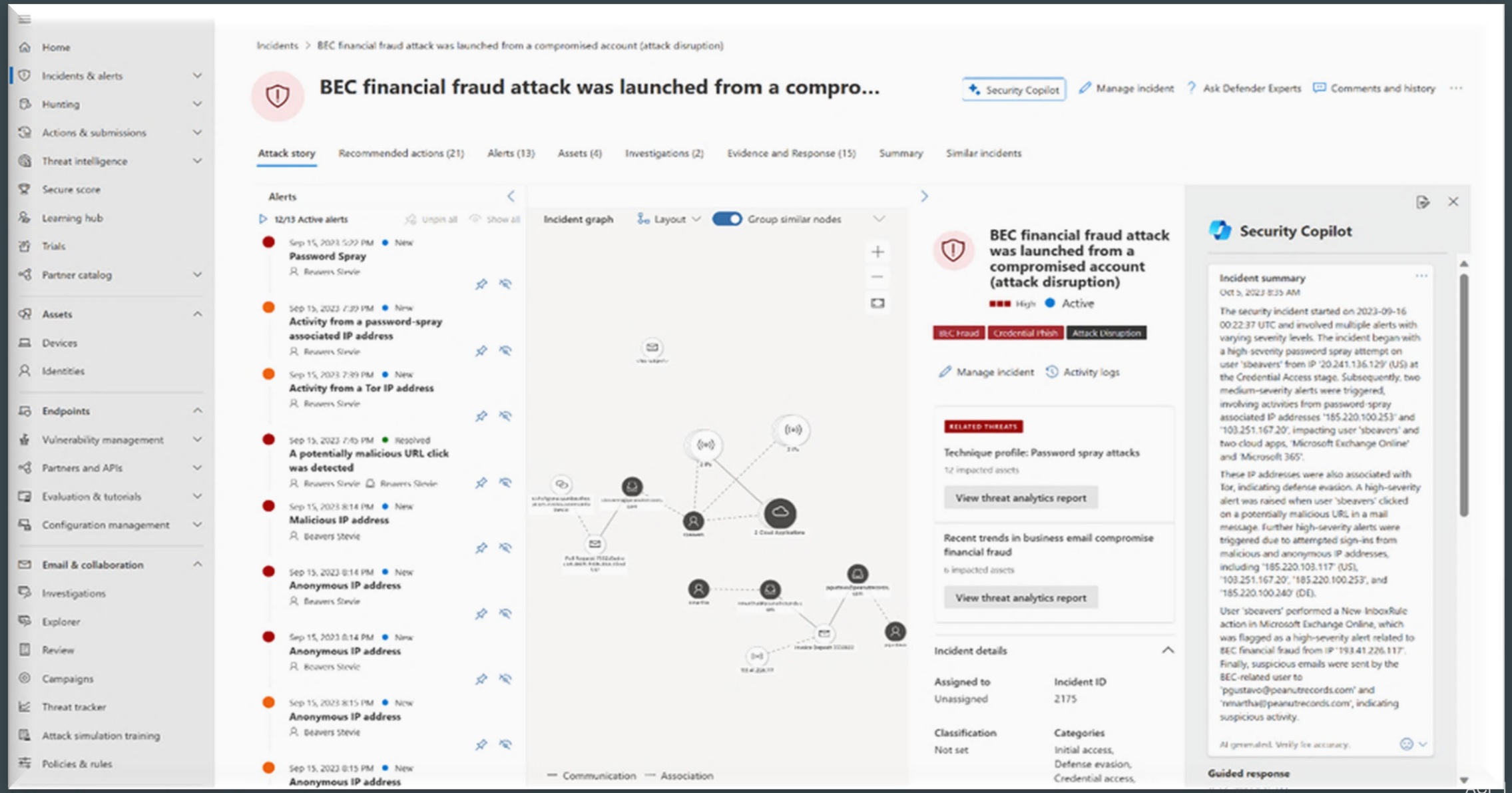


Quellen: https://www.microsoft.com/

Copilot für Security

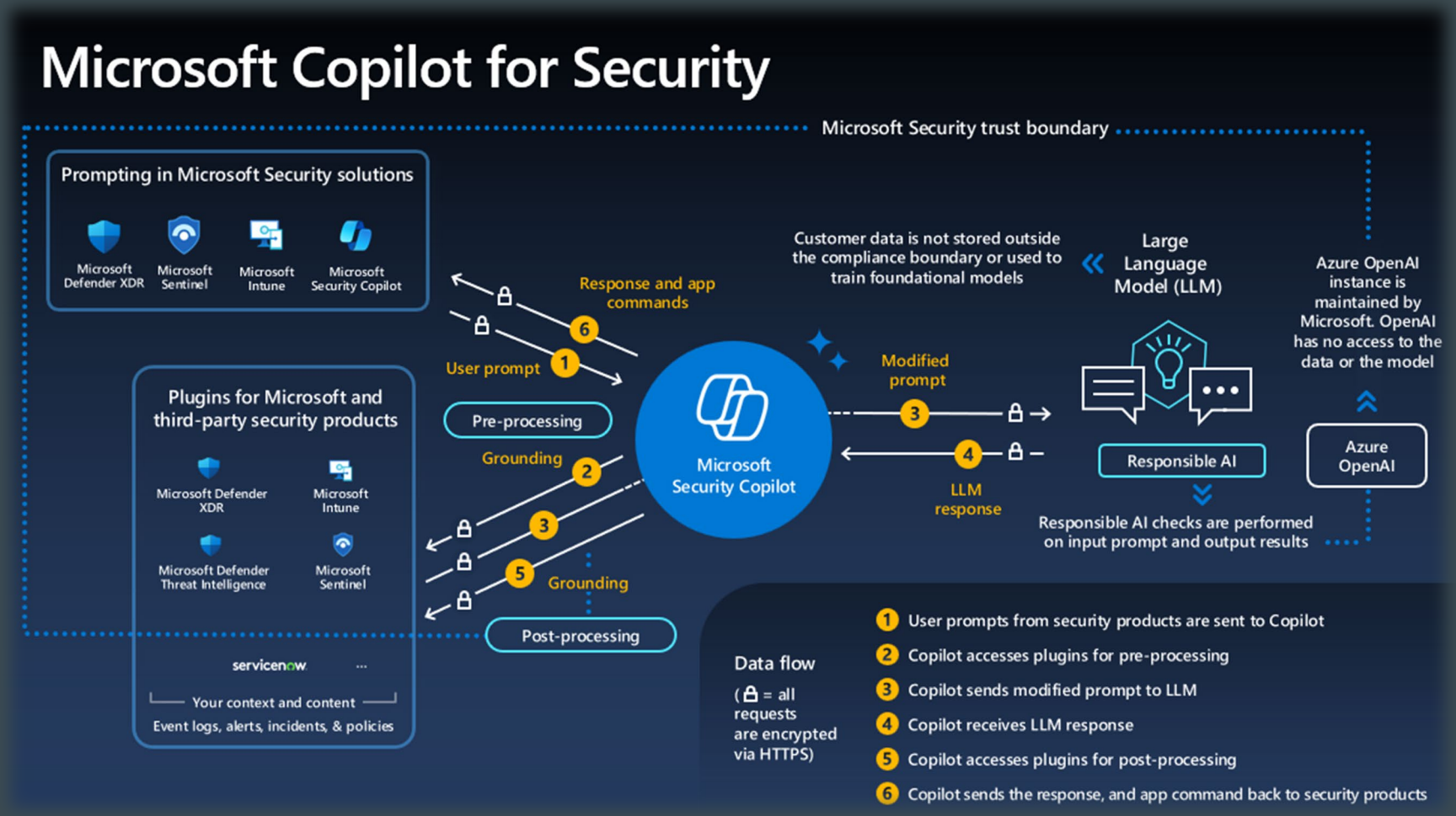
Quellen: https://www.microsoft.com/

Copilot für Security



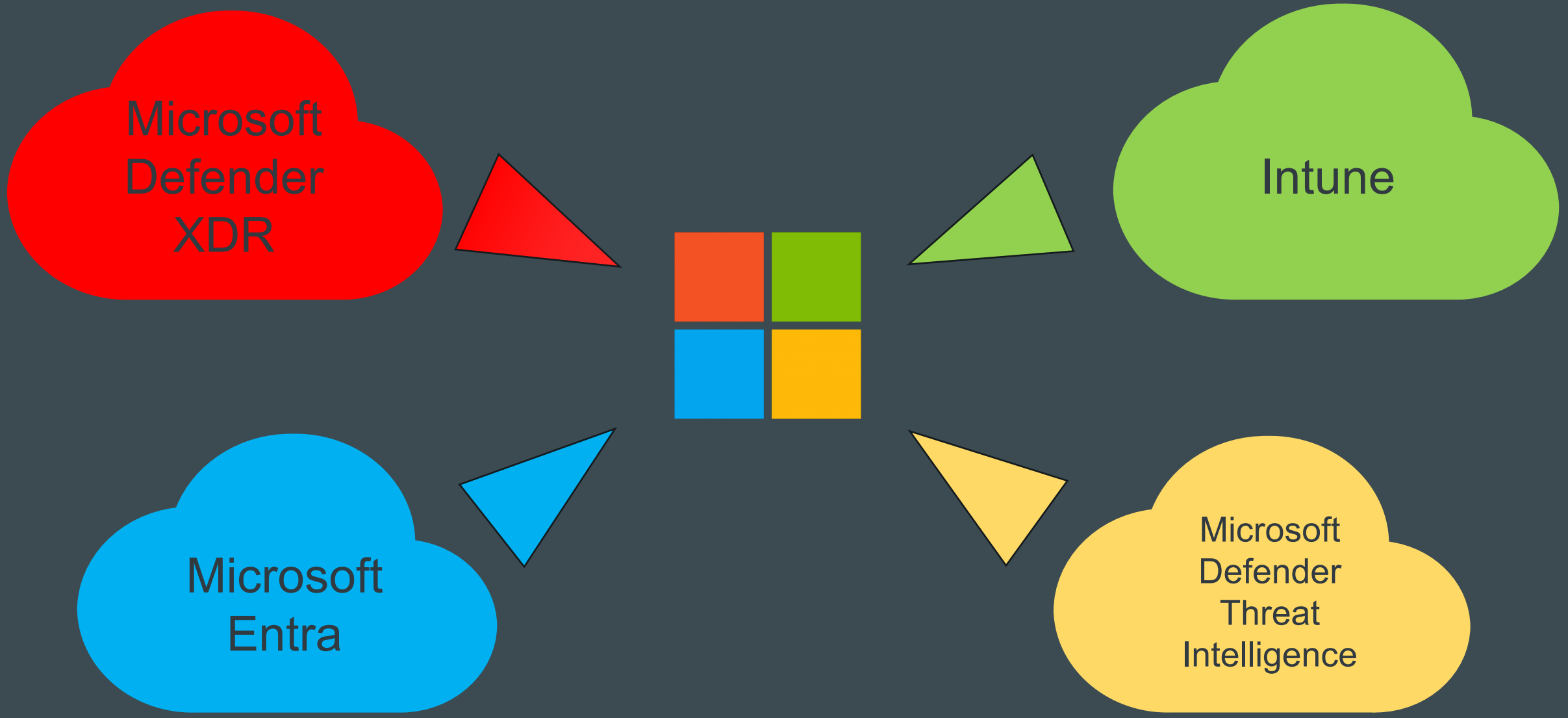
Quellen: https://www.microsoft.com/

Copilot für Security



Quellen: https://www.microsoft.com/

Copilot für Security



Hand in Hand mit der KI

- Erhöhte Effizienz
- Einfache Integration
- Schutz for Insider-Bedrohungen
- Proaktive Sicherheitsmaßnahmen
- Automatisierte Bedrohungserkennung und -abwehr

Empfehlungen

- Patchmanagement
- Social-Engineering-Prävention
- Nutzung der KI für Verteidigungsmaßnahmen
- Verbesserung der Angriffserkennung
- Aufbau einer resilienten IT-Infrastrukur

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

IT for innovators.