

IT Security Architecture

-

Neue Ansätze und Lösungen





Manuel Götz

Consultant
CCNP Security

IT for
innovators.



Alexander Knauff

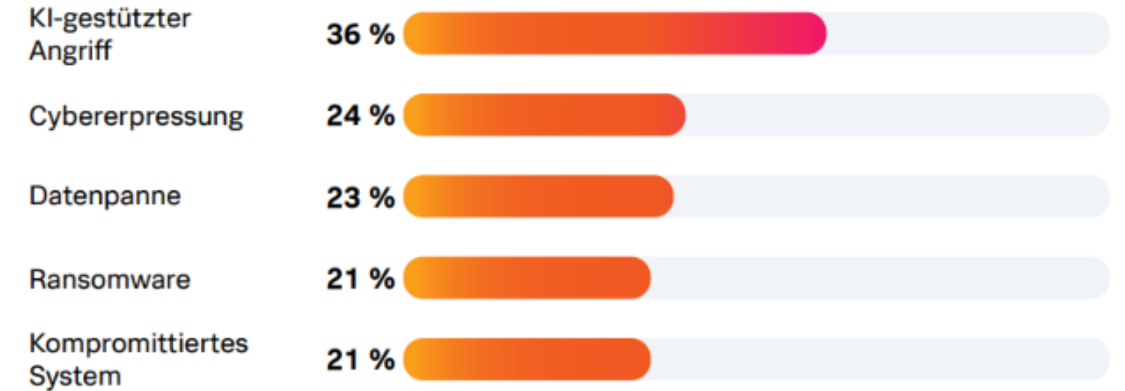
Senior Support Engineer

IT for
innovators.

Lagebericht Security 2024



Welche Cyberangriffe bereiten die meisten Sorgen?



Die häufigsten Bedrohungsvektoren

38 %

Fehlkonfigurierte Systeme



31 %

Schwachstellen in selbst entwickelten Apps



30 %

Zero-Day-Schwachstellen



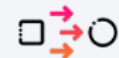
29 %

Bekannte Software-Schwachstellen



28 %

Seitwärtsbewegung



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





Secure Service Edge

SSE



Project Timeline





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

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



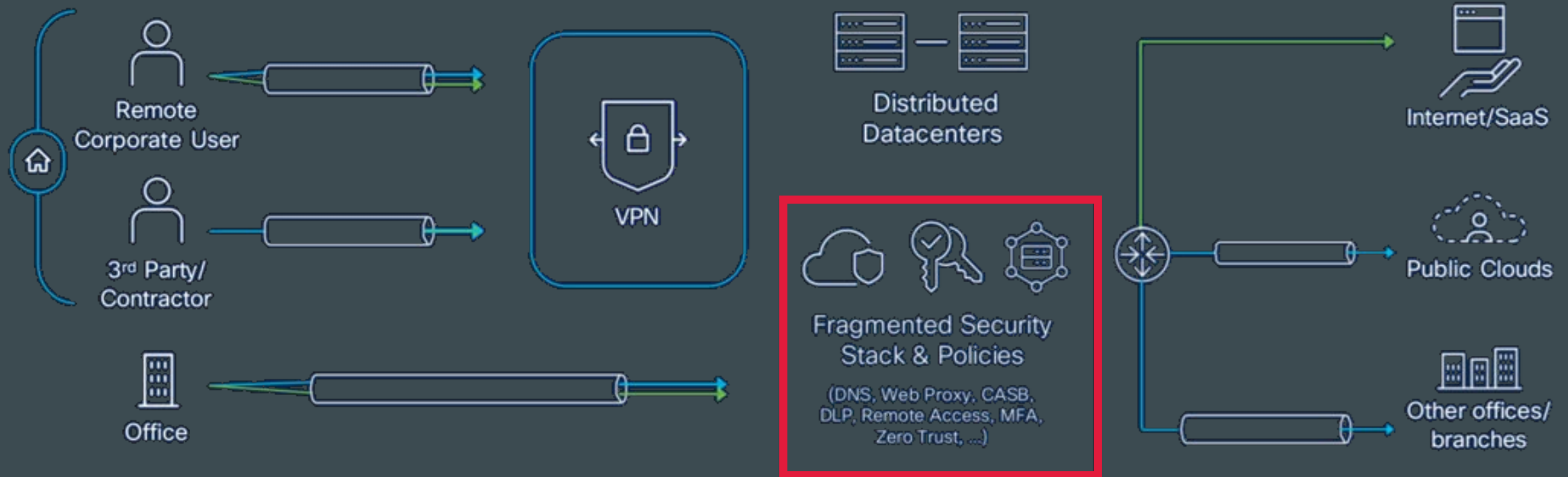
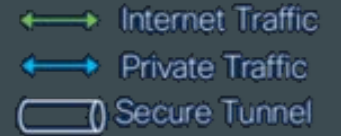
„Die IT-Security steht der Produktivität der Mitarbeiter im Weg!“

Homeoffice



Herausforderung

Eine Architektur, die nie für hybrides Arbeiten konzipiert wurde!



Use Cases unserer Kunden

Secure Internet Access



Internet
apps



SaaS
apps



Secure Private Access



Private
apps



Security Service Edge (SSE)

Secure Access
from anywhere to
everywhere

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

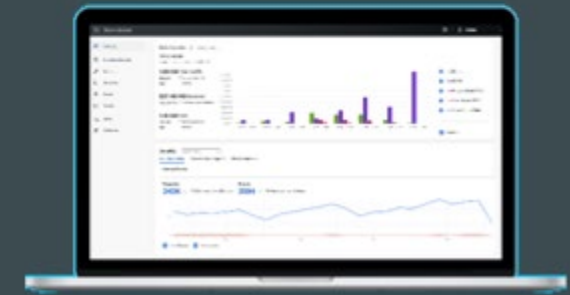


Introducing Cisco Secure Access

Proven cloud-native security converged into one service



Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

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

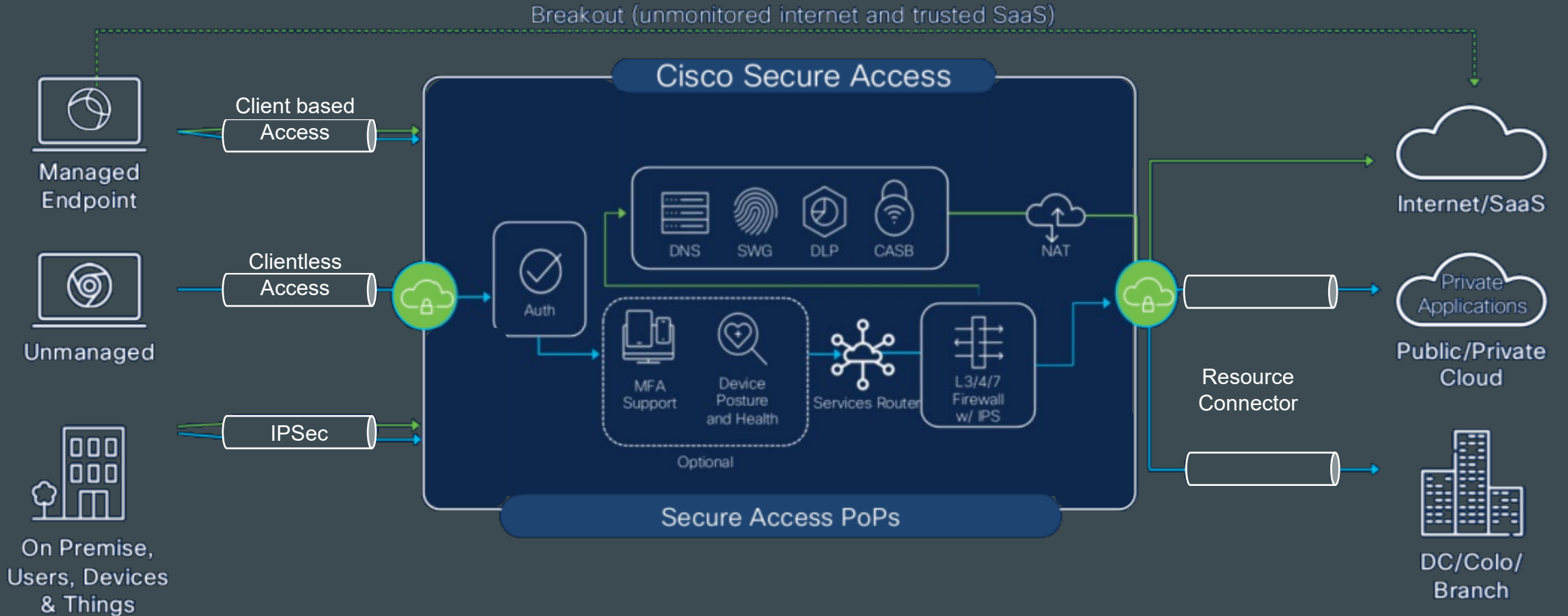
ISE Integration

Apple Private Relay

ThousandEyes
Digital Experience Monitoring (DEM)

SD-WAN Integration

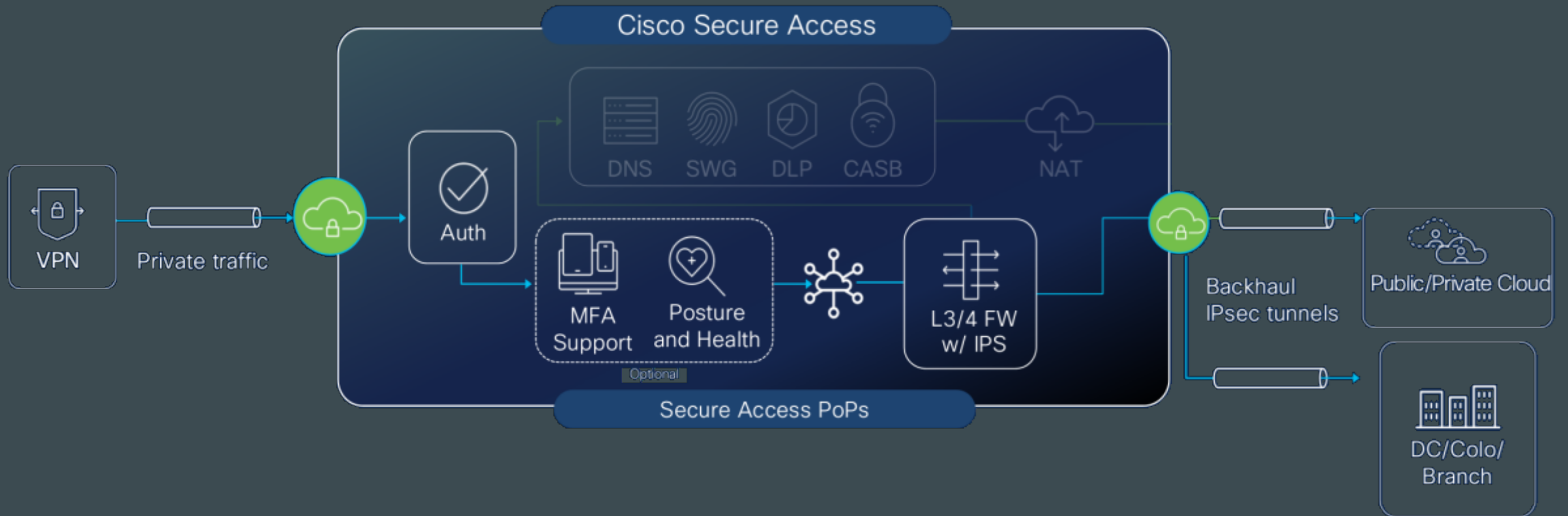
Architecture Overview



Users

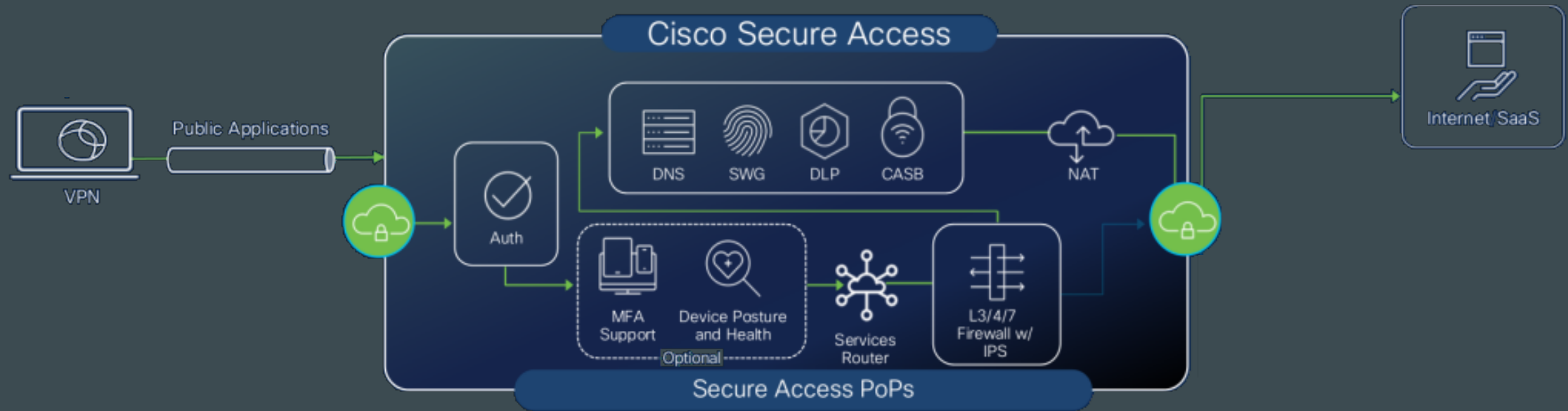
How

Apps



Benefits

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



Capabilities

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

Unified Policy!

Policy Rule Defaults and Global Settings

Search by Filter Add Rule

16 Rules

#	Rule name	Rule type	Actions	Sources	Destinations	Security Control	Status
1	Eng2Internet-Allow	Internet Access	Allow	Engineering (tmelabs.com)Engineering	News +1	IPS, Web, Tenant	Enabled
2	Eng2Internet-Warn	Internet Access	Warn	Engineering (tmelabs.com)Engineering	BH-Warn	IPS, Web	Enabled
3	Eng2Internet-Block	Internet Access	Block	Engineering (tmelabs.com)Engineering	BH-Block	Web	Enabled
4	Health App	Private Access	Allow	Eng1 (eng1@tmelabs.com)	Health DB	-	Disabled
5	Finance To Finance Resources	Private Access	Allow	Finance (tmelabs.com)Finance	Finance Portal	-	Enabled
6	Eng to Eng Resources	Private Access	Allow		WS-Jira	-	Enabled
7	BH-Jira-ZTA	Private Access	Allow		WS-Jira	-	Enabled
8	BH-BAP	Private Access	Allow		Jira-BAP	IPS	Enabled
9	Test SaML	Internet Access	Block		Internet destination	Web	Disabled
10	block IP App	Private Access	Block		IP-VPN	-	Disabled

Rows per page 10 < 1 2 >

Default Rules

Rule name	Action	Sources	Destinations	Security Control	Posture
Default Rule	Block	Any	Any private application	-	-
Default Rule	Allow	Any	Any Internet destination	IPS, Web, Tenant	-

DNS, FWaaS, SWG

ZTNA & RAVPN, Private Access



- Overview
- Experience Insights**
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

Experience Insights

Last updated Jun 10, 2021 19:33

By integrating with Thousand Eyes technology, you can have a clear view of how well your users, applications, and networks are performing. Want to know more? [Launch ThousandEyes](#) to access detailed information, including a look back at historical data for various time periods. [Help](#).

Endpoint performance overview ⓘ

Performance health summary ⓘ 96 total

3 Unhealthy 🚫 4 At risk ⚠️ 89 Healthy 🟢

Endpoints ⓘ 120 total

96 Connected to the Cisco Secure Access cloud 🟢

Performance health events ⓘ

Search Health status Device Location 0 devices [Reset all](#)

United Kingdom 5 min ago

2 Unhealthy 🚫 2 At risk ⚠️ 4 Healthy 🟢

New York, US 5 min ago

0 Unhealthy 🚫 0 At risk ⚠️ 50 Healthy 🟢

Romania 5 min ago

0 Unhealthy 🚫 2 At risk ⚠️ 4 Healthy 🟢



Endpoints ⓘ

User name	Health status	Device	Latency (ms)	Jitter (ms)	Loss (%)	WiFi (dB)	CPU (%)	Memory (%)	Location
Lee Wetherspoon	Unhealthy 🚫	PC Windows 10.X.X	3.0	3.0	3.0	72	43	56	United Kingdom
Anna Spearing	Unhealthy 🚫	PC Windows 10.X.X	3.0	3.0	3.0	72	32	35	United Kingdom
Jinv Johnson	Unhealthy 🚫	PC Windows 10.X.X	1.0	1.0	1.0	72	31	34	New York, US

• **Close background applications:** Even if you are not using them, applications on your device are using precious resources. Before your meeting, close any applications and browser sessions that you are not using for a better experience.

Digital Experience Monitoring

Identifizierung und Lösung von Problemen

Top 20 SaaS Application Health

Common SaaS applications Performance ⓘ

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



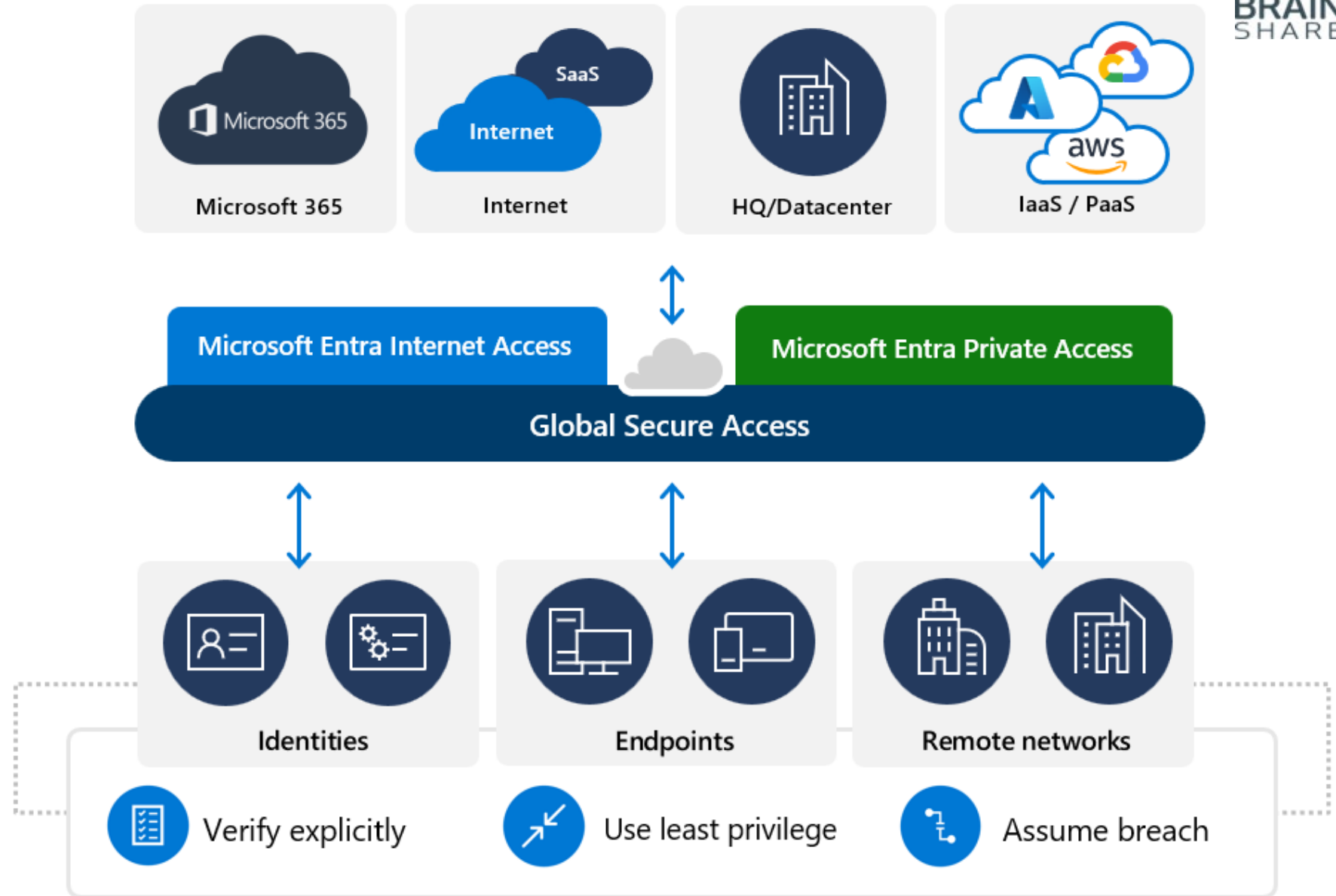
Microsoft Global Secure Access





Global Secure Access

Technischer Überblick

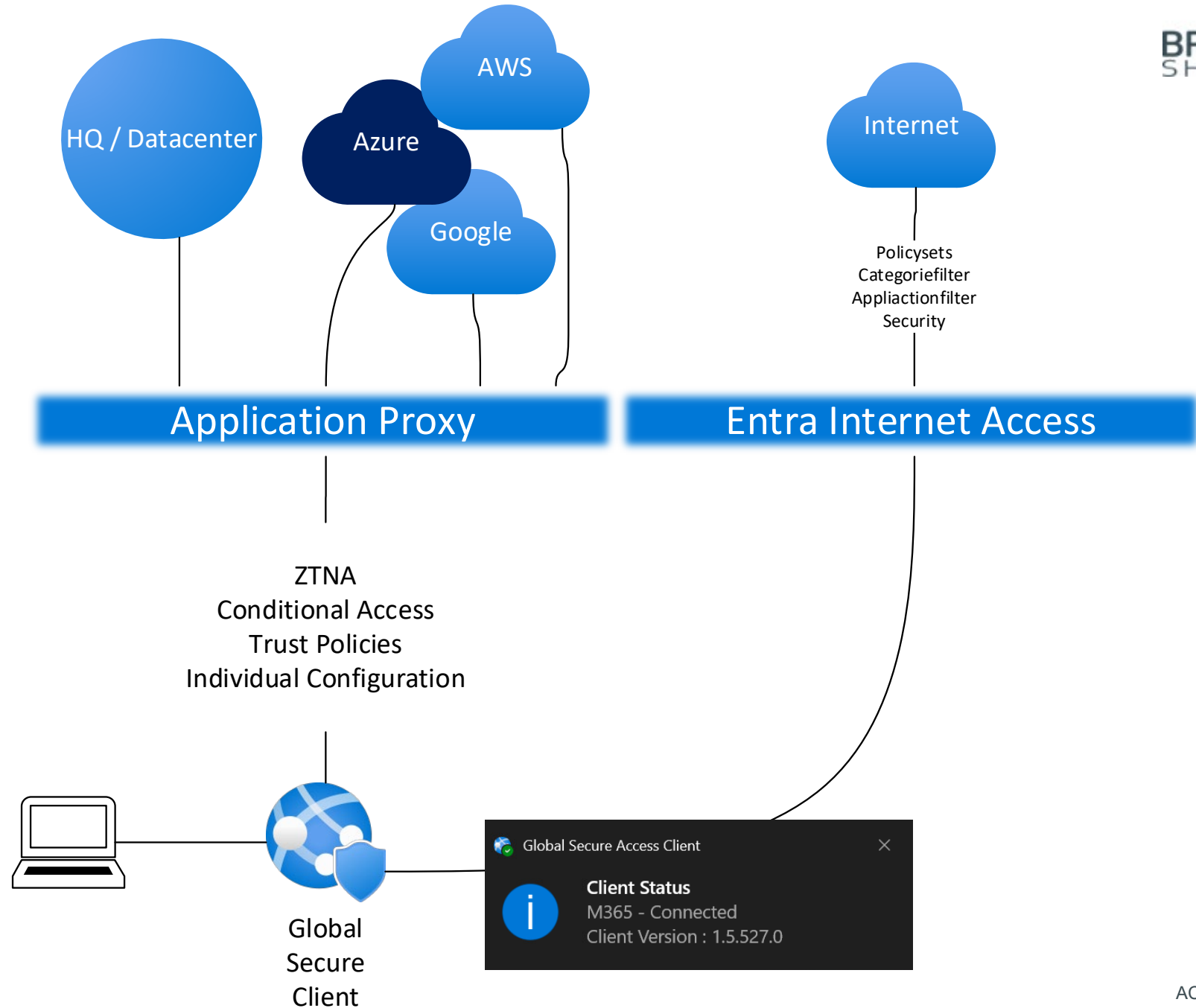




Global Secure Access

Global Secure Access Client

Firmennetz
jederzeit und überall

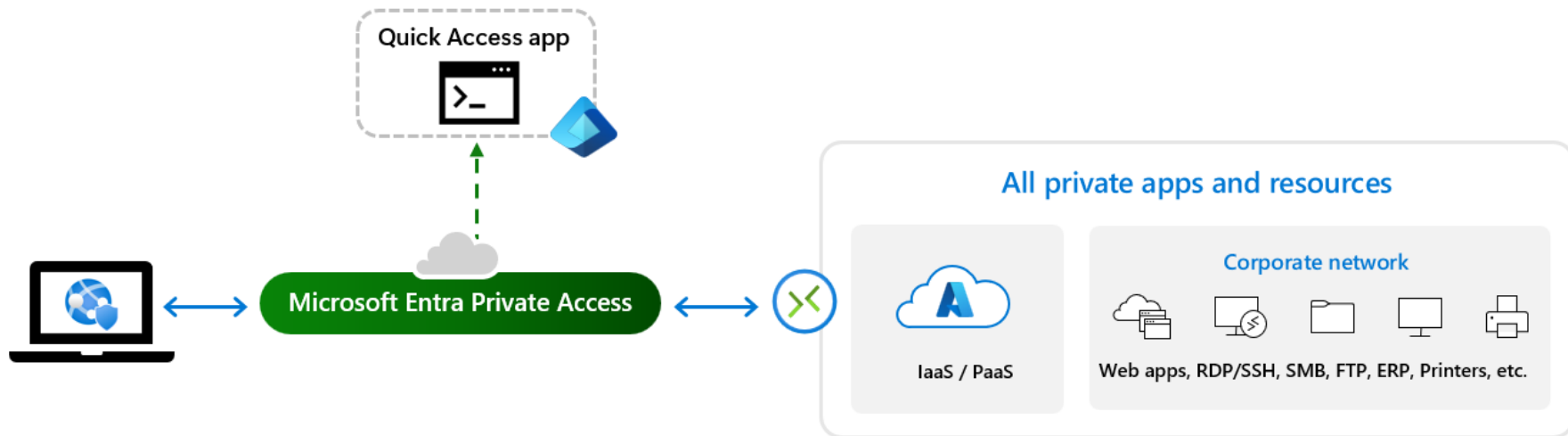
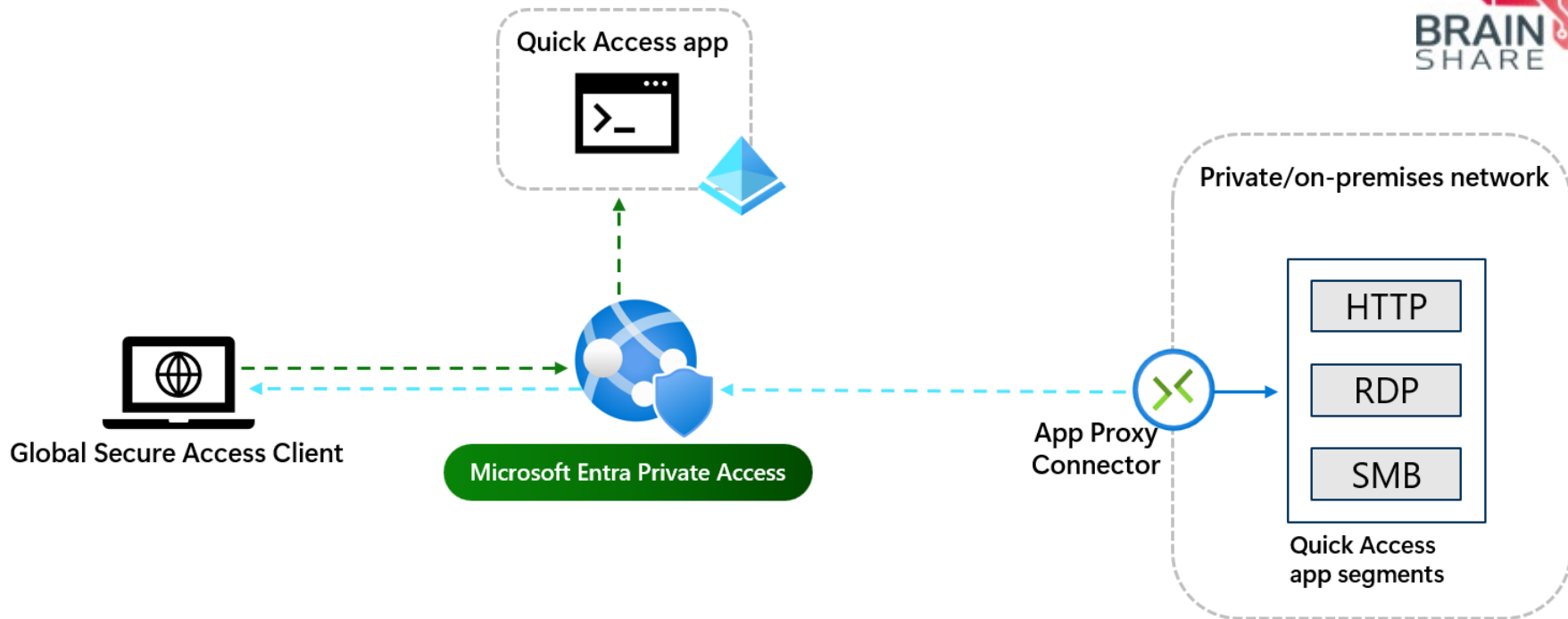




Global Secure Access

Firmennetz

Zugriff von extern





Global Secure Access

Ein Dashboard

Alle Daten in einer Plattform

Microsoft Entra admin center Search resources, services, and docs (G+)

Home > Woodgrove > Woodgrove

Welcome to Global Secure Access

Secure access and improve visibility to the internet, Microsoft 365, SaaS, and private apps. [Learn more about Global Secure Access](#)

[Get Started with the dashboard](#) [Got feedback?](#)

Last 24 hours

Global Secure Access snapshot

Traffic type : All

The Global Secure Access snapshots provides quick access to the users, devices, and destinations with network traffic captured by Microsoft Entra Private Access and Microsoft Entra Internet Access.

Out of 846 devices, 5 have the Global Secure Access Client installed: 0.6%

Device status

Active devices
5 ▲ 25% in the last 24 hours

The number of distinct active devices that signed in to other tenants in the last 24 hours

Alerts and notifications

1 notifications

Alert name

The number of users accessing external tenants has increased [Check cross-tenant access settings](#)

Top used destinations

Review the top-used destinations by traffic type.

All **Microsoft 365** Internet Access ...

Sort by : Transactions

login.microsoftonline.com	3K
aps.globalsecureaccess.microsoft.com	1.7K

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

Einfluss von KI auf die Cyberbedrohungslandschaft

10.04.2024



Bundesamt
für Sicherheit in der
Informationstechnik

1 Einleitung

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

IT for
innovators.



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



The image shows a close-up of a textured, light-colored surface, possibly a book cover or folder, featuring the Cisco logo. The logo consists of a series of seven vertical bars of varying heights, arranged in a slightly curved line. Below the bars, the word "CISCO" is printed in a bold, red, sans-serif font. To the right of the word "CISCO", the letters "TM" are printed in a smaller, red font. Overlaid on the center of the image is the text "Cisco Security AI" in a white, sans-serif font.

Cisco Security AI

CISCOTM

AI Assistant in der Firewall

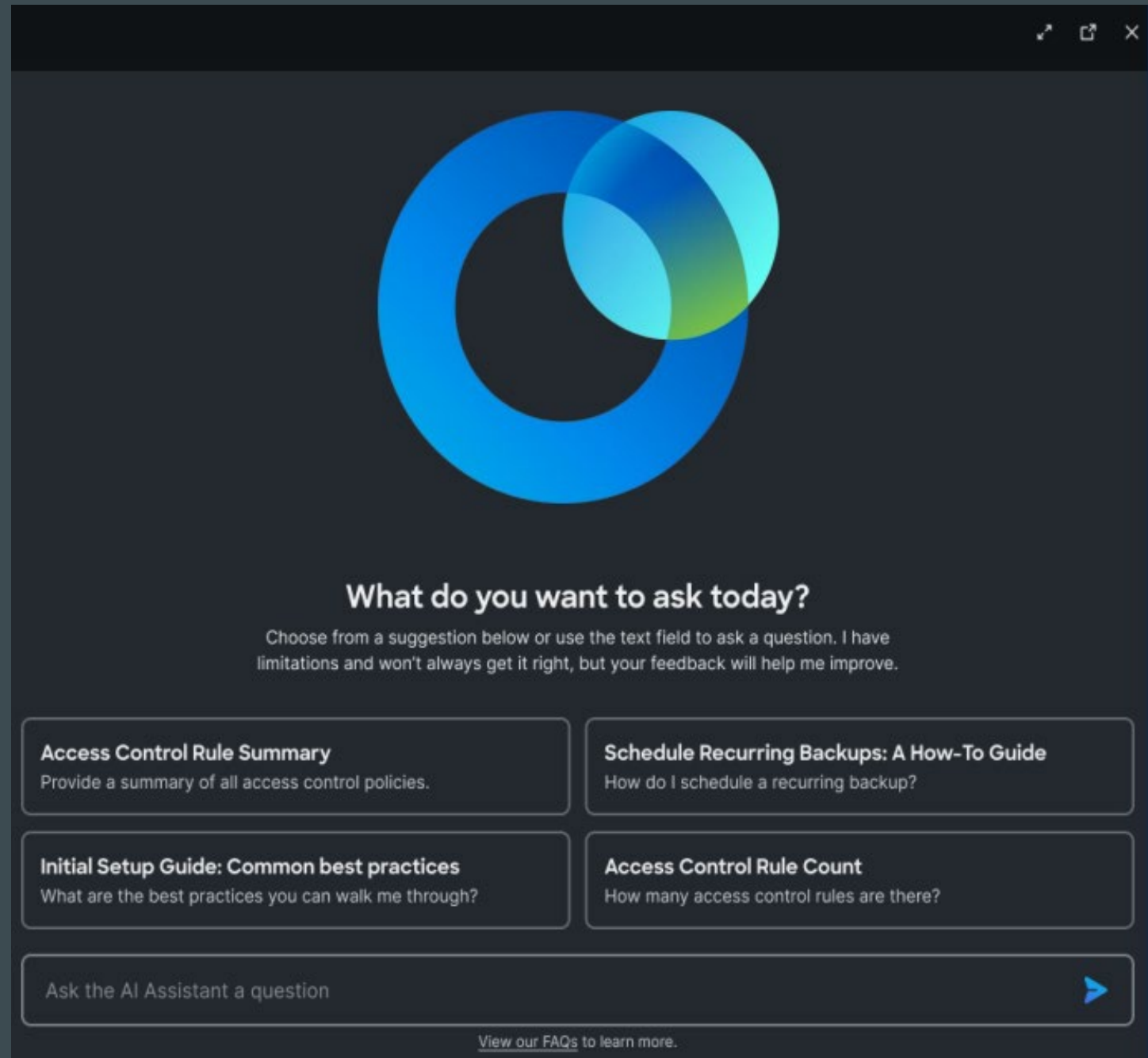


- Troubleshooting beschleunigen
- Schneller agieren
- Visibilität erhöhen
- Best Practises umsetzen

IT for
innovators.

AI Assistant in der Secure Firewall

IT for
innovators.



What do you want to ask today?


Choose from a suggestion below or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

Access Control Rule Summary
Provide a summary of all access control policies.

Schedule Recurring Backups: A How-To Guide
How do I schedule a recurring backup?

Initial Setup Guide: Common best practices
What are the best practices you can walk me through?

Access Control Rule Count
How many access control rules are there?

Ask the AI Assistant a question 

[View our FAQs](#) to learn more.

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

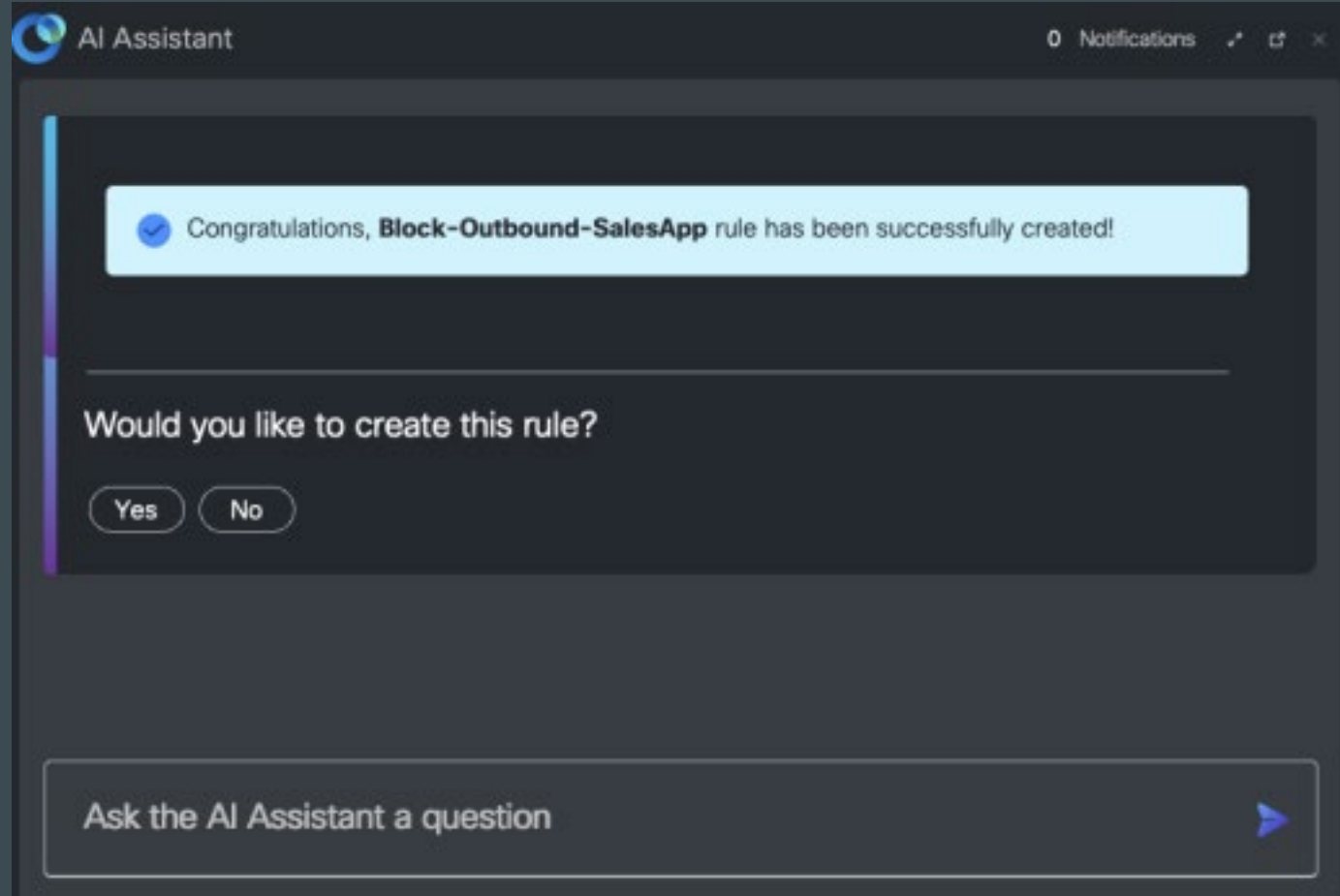
AI Assistant in XDR

The screenshot displays the Cisco XDR AI Assistant interface. The chat window on the left shows a user asking, "Who are the owners associated with these endpoints?" and "What endpoints were affected by this malicious file?". The AI Assistant responds with a list of endpoints: E2E-DataLake-Internet1, DESKTOP-2ER967Q, E2E-Win10-x64-G, and Desktop-Win53. The user then asks, "How do you want to address this incident?", and the AI Assistant suggests, "Quarantine the compromised systems." The right pane shows a network diagram with nodes representing endpoints and files, connected by "Behavioral relationship" lines. A red dashed circle highlights a cluster of nodes, including "Malicious SHA-256" and "263efd9cd6...".

IT for
innovators.

- Direkte Weiterleitung zum CDO mit allen Angriffsinformationen

AI Assistant in XDR



- Blockregel wird vorgeschlagen und kann direkt erstellt werden

IT for
innovators.

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

AI Assistant in XDR

The screenshot displays the Duo console interface. On the left, an AI Assistant chat window is open, showing a conversation about access policies for the user group 'Inn-vendor'. The assistant provides information about 3 Access Control Policies and 10 Access Control Rules, with 4 rules related to sensitive data and 2 rules related to internal application access. Below the chat is a table of rules.

Rule	Associated policy	Status	Sources	Local IP
<input type="checkbox"/> FW_NorthAmerica_DataTX	XYZ_ABC	Allow	All employees	Internal resources +23
<input type="checkbox"/> FW_NorthAmerica_DataTX	XYZ_ABC	Allow	All employees	Internal resources +23
<input type="checkbox"/> FW_NorthAmerica_DataTX	XYZ_ABC	Block	All employees	Internal resources +23
<input type="checkbox"/> FW_NorthAmerica_DataTX	XYZ_ABC	Allow	All employees	Internal resources +23
<input type="checkbox"/> FW_NorthAmerica_DataTX	XYZ_ABC	Block	All employees	Internal resources +23

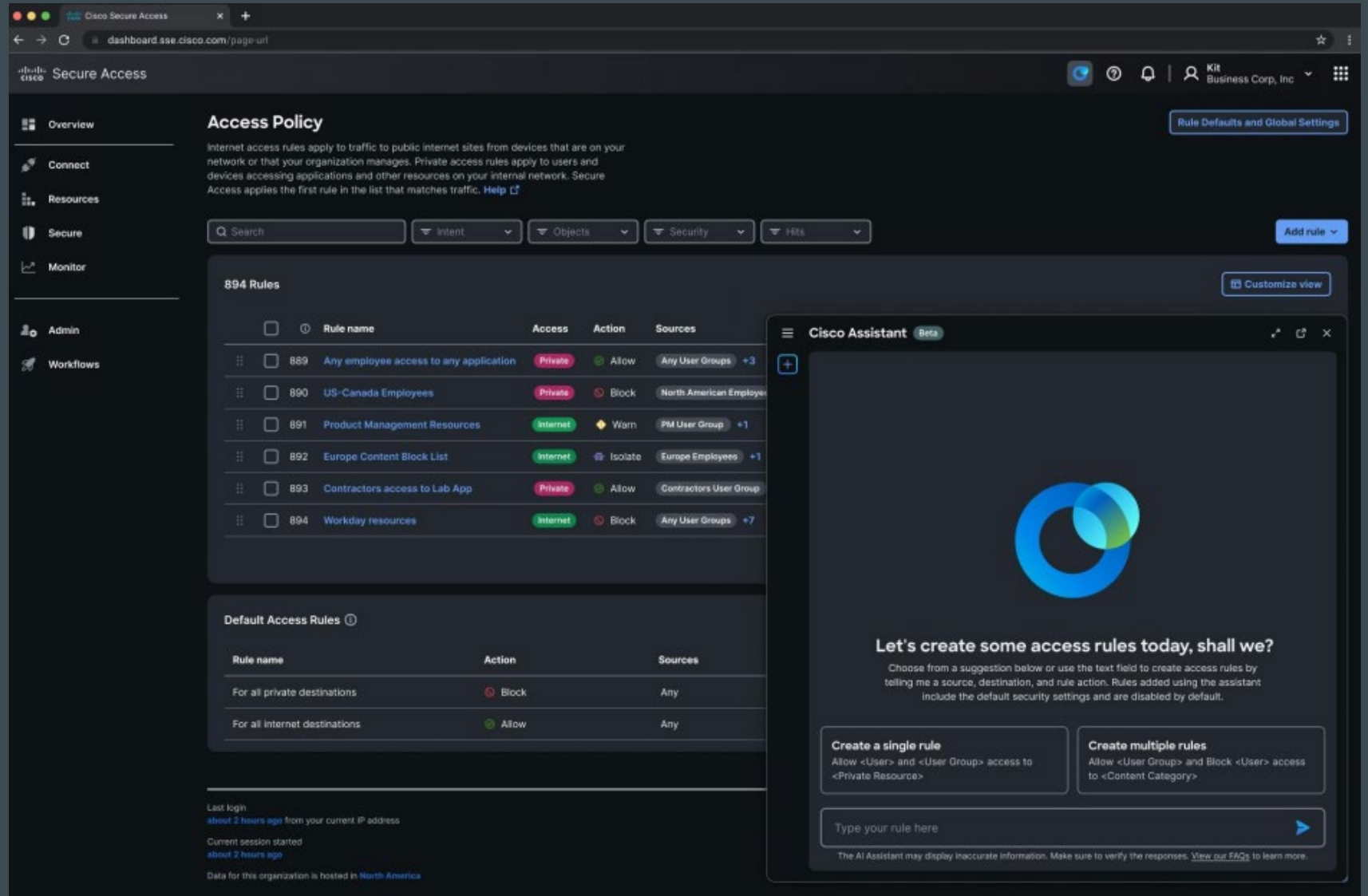
On the right, the dashboard shows a 1.3% increase in change in the last 7 days. Below this are several metrics: 22 Administrators, 4.4k 2FA Devices, 73 Groups, and 114 New Trust Monitor Security Events, including 13 Priority Events. At the bottom right, there is a bar chart showing activity over time, with a peak around 6 AM on Monday, August 21st.

IT for
innovators.

Policy administration beschleunigen

AI Assistant in Secure Access

IT for
innovators.



The screenshot displays the Cisco Secure Access dashboard. The main section is titled "Access Policy" and contains a list of 894 rules. Below this, there is a "Default Access Rules" section with two entries:

Rule name	Action	Sources
For all private destinations	Block	Any
For all Internet destinations	Allow	Any

Overlaid on the right side of the dashboard is the "Cisco Assistant" interface, which prompts the user to "Let's create some access rules today, shall we?". It offers two options: "Create a single rule" and "Create multiple rules". Below these options is a text input field labeled "Type your rule here" and a blue arrow button. A disclaimer at the bottom of the assistant window states: "The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more."

AUGMENT

Korrelierung und Überwachung
von Informationen und Events
mit maschineller
Geschwindigkeit



Korrelation von 555 Milliarden Security Events pro Tag

AI Powered Detection

Talos Powers The Cisco Portfolio With Intelligence

TALOS



500

threat researchers



AI

powered algorithms



550B

security events observed daily

IT for
innovators.

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

Encrypted Visibility Engines (EVE)

IT for
innovators.



AUTOMATE

Automatisierung komplexer
Arbeitsabläufe die IT-Administratoren
in jeglicher Hinsicht unterstützen

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

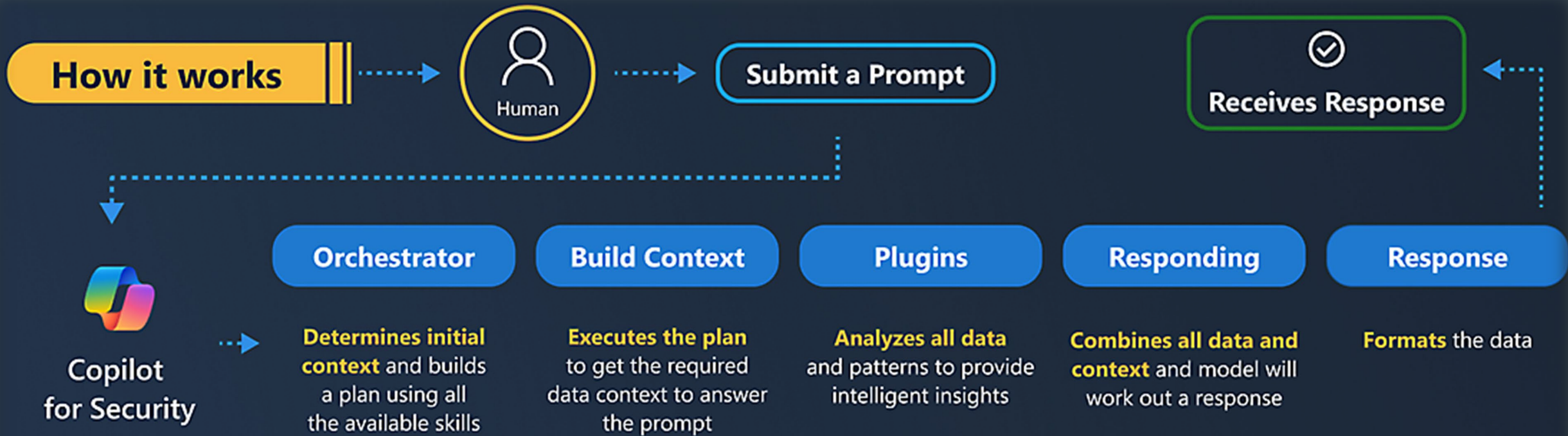
Autonomous Actions



IT for
innovators.



Copilot für Security





Copilot für Security



Security Copilot



Show me events from compromised
Accounts





- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Attack simulation training
- Policies & rules

Incidents > BEC Financial fraud attack was launched from a compromised account (attack disruption)

Security Copilot
Manage incident
Ask Defender Experts
Comments and history

BEC financial fraud attack was launched from a compro...

Attack story
Recommended actions (21)
Alerts (13)
Assets (4)
Investigations (2)
Evidence and Response (15)
Summary
Similar incidents

Alerts

12/13 Active alerts

- Sep 15, 2023 5:22 PM ● New
Password Spray
Beavers Stevie
- Sep 15, 2023 7:29 PM ● New
Activity from a password-spray associated IP address
Beavers Stevie
- Sep 15, 2023 7:39 PM ● New
Activity from a Tor IP address
Beavers Stevie
- Sep 15, 2023 7:40 PM ● Resolved
A potentially malicious URL click was detected
Beavers Stevie
- Sep 15, 2023 8:14 PM ● New
Malicious IP address
Beavers Stevie
- Sep 15, 2023 8:14 PM ● New
Anonymous IP address
Beavers Stevie
- Sep 15, 2023 8:14 PM ● New
Anonymous IP address
Beavers Stevie
- Sep 15, 2023 8:15 PM ● New
Anonymous IP address
Beavers Stevie
- Sep 15, 2023 8:15 PM ● New
Anonymous IP address
Beavers Stevie
- Sep 15, 2023 8:15 PM ● New
Anonymous IP address
Beavers Stevie

Incident graph

Layout Group similar nodes

Communication Association

BEC financial fraud attack was launched from a compromised account (attack disruption)

■ High ● Active

BEC Fraud Credential Phish Attack Disruption

Manage incident Activity logs

RELATED THREATS

Technique profile: Password spray attacks
12 impacted assets

[View threat analytics report](#)

Recent trends in business email compromise financial fraud
6 impacted assets

[View threat analytics report](#)

Incident details

Assigned to	Incident ID
Unassigned	2175
Classification	Categories
Not set	Initial access, Defense evasion, Credential access,

Security Copilot

Incident summary
OCT 5, 2023 8:25 AM

The security incident started on 2023-09-16 00:22:37 UTC and involved multiple alerts with varying severity levels. The incident began with a high severity password spray attempt on user 'sbeavers' from IP '20.241.136.129' (US) at the Credential Access stage. Subsequently, two medium-severity alerts were triggered, involving activities from password-spray associated IP addresses '185.220.100.253' and '103.251.167.20', impacting user 'sbeavers' and two cloud apps, 'Microsoft Exchange Online' and 'Microsoft 365'.

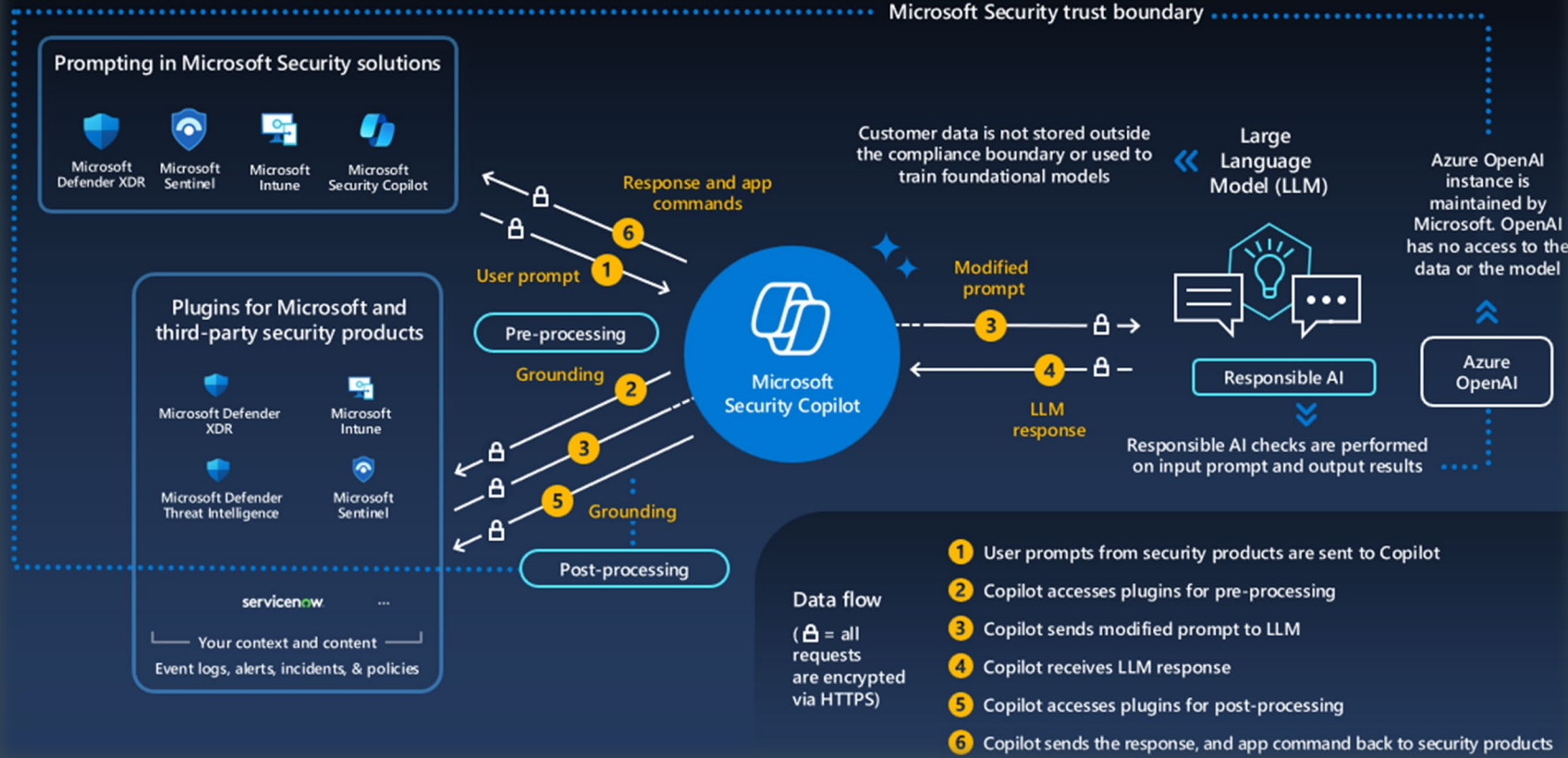
These IP addresses were also associated with Tor, indicating defense evasion. A high-severity alert was raised when user 'sbeavers' clicked on a potentially malicious URL in a mail message. Further high-severity alerts were triggered due to attempted sign-ins from malicious and anonymous IP addresses, including '185.220.103.117' (US), '103.251.167.20', '185.220.100.253', and '185.220.100.240' (DE).

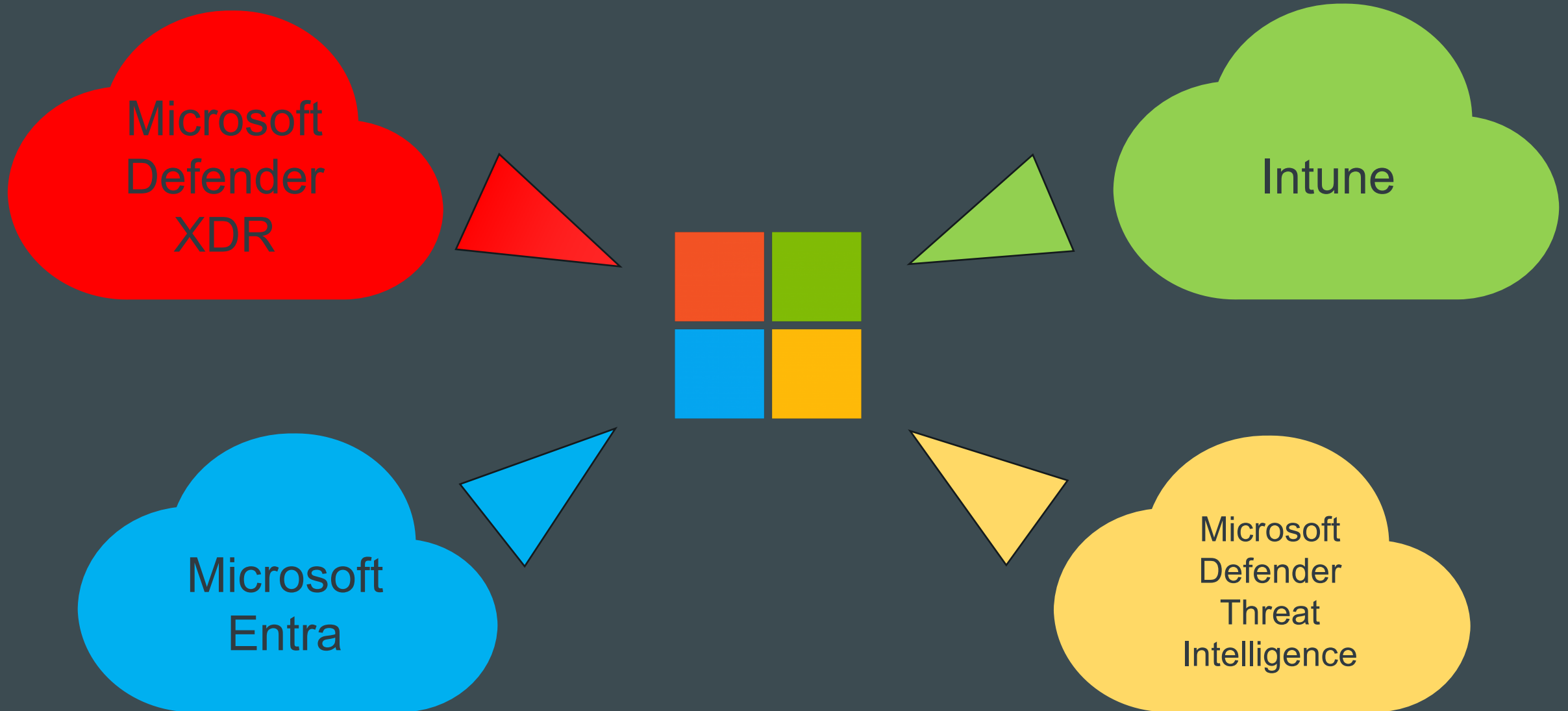
User 'sbeavers' performed a New InboxRule action in Microsoft Exchange Online, which was flagged as a high-severity alert related to BEC financial fraud from IP '193.41.226.117'. Finally, suspicious emails were sent by the BEC-related user to 'pgustavo@peanutrecords.com' and 'remartha@peanutrecords.com', indicating suspicious activity.

AI generated. Verify for accuracy.



Microsoft Copilot for 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-Infrastruktur





**Vielen Dank für Ihre
Aufmerksamkeit**

Fragen?

**IT for
innovators.**