Cisco Security

Simplified security to meet you anywhere

Sebastian Weigerstorfer
Security Solutions Engineer

InfotechDay24

Cisco investiert in Sicherheit

"If it´s connected, you´re protected"

2007 — IronPort Systems
Top leader of contents security

2009 — ScanSafe
Top leader of cloud-based web security

2013 — CO|SE Cognitive Security
Applies artificial intelligence techniques to detect advanced cyber threats

2014 — ThreatGRID Malware Threat Intelligence Platform
- Leading dynamic malware analysis (Sandbox)
- Currently integrated to Endpoint

2015 — Sourcefire
- Snort®, ClamAV®, Open Source projects founder
- VRT world-class research
- Top leader of IPS

2015 — Neohapsis Securing the Mobile Economy
- Top leaders of security advisory services
- Provides risk management and compliance to Fortune 500 customers

2015 — Lancope
- Leading security analytics platform to defend against advanced cyber threats

2015 — OpenDNS
Cloud-based DNS security services

2016 — CloudLock
Leading cloud security platform that provides visibility and control for SaaS, IaaS and PaaS

2017 — Observable Networks
Cloud-based network forensics and visibility

2018 — Duo
Leader in two factor authentication, endpoint remediation and secure single sign-on

2022 — Kenna Security
Risk-based vulnerability management software

2023 — Accedian
Lightspin
End-to-end cloud security posture management across cloud-native resources

2023 — Valtix
Cloud network security for multi cloud workloads

2023 — Armorblox
Predictive and generative AI across our product portfolio

2023 — Intent to acquire: Splunk, wgtwo

2023 — Isovalent

2023 — Smartlook
Session recordings with event-based analytics to analyze end-user digital behavior

2023 — Dort
Identity Threat Detection and Response technology

2023 — Sam Knows
Expand ThousandEyes' industry-leading view of global internet health

2023 — Code BGP
Deepens ThousandEyes' BGP Capabilities

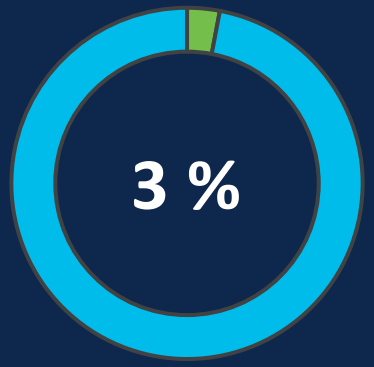
2007 2009 2013 2014 2015 2016 2017 2018 2022 2023 ▶▶▶

Warum tun wir das ?

Die Lage ist ernst: Jeden kann es treffen

Unzureichend vorbereitete und übertrieben selbstbewusste Unternehmen/Behörden

Cisco Cybersecurity Readiness Index | 2024



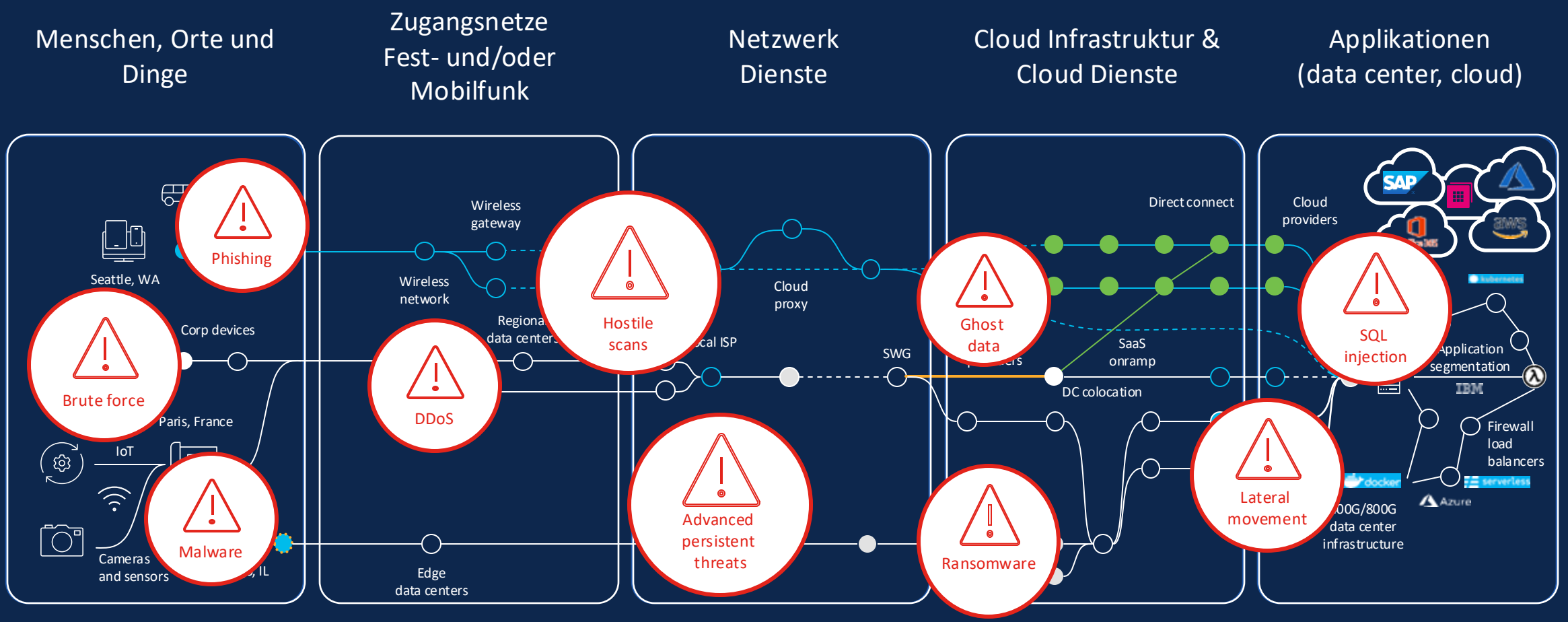
aller Unternehmen sind bestmöglich vorbereitet

Die Folgen …

- Finanzielle Risiken
- Produktionsausfälle
- Reputationsverlust
- Datenverlust
- Persönliche Risiken

Was hat sich verändert ?

Home Office, Cloud und SD-WAN bedeutet ...



Die Angriffsfläche ist gewachsen!

Die meisten Angriffe verwenden eine Abfolge wie diese...

Eine gut angepasste und personalisierte E-Mail veranlasst den Benutzer zum Klicken...

Welche zu einer fragwürdigen Website geht ...

Was dazu führt, dass ein seltsamer Prozess lokal auf dem Gerät des Benutzers erstellt wird...

Dieser Prozess wird sich mit einer anderen Maschine verbinden oder direkt auf ihre Daten zugreifen

T1566: Spear Phishing

T1055: Process Injection

T1189: Drive-by Compromise

T1087: Account Discovery: Domain account

T1210: Exploitation of Remote Services

T1048: System Network Connections Discovery

Vendor A	Vendor B	Vendor C	Vendor D	Vendor E

Zwei Kernfragen zur Nutzung von KI

1

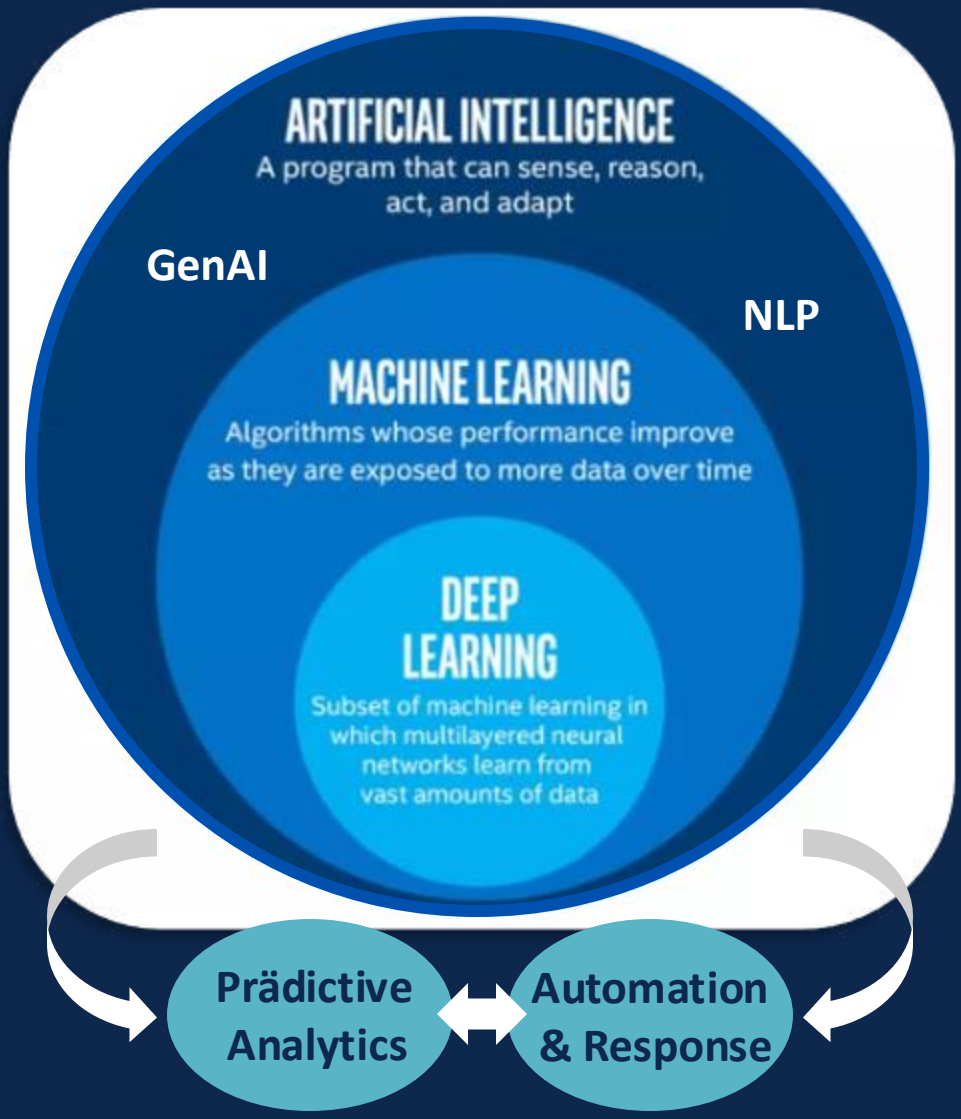
Wozu will ich KI nutzen...

...welche Anwendungsfälle (Use Cases) ?

...welche KI und Methoden ?

High-Level Überblick – Künstliche Intelligenz (KI)

- **KI** steht für **Künstliche Intelligenz** (engl. Artificial Intelligence (AI)) und bezieht sich auf die **Entwicklung von Computern oder Maschinen**, die **menschenähnliche Intelligenz aufweisen** sollen
- **ML** steht für **Maschinelles Lernen** (Machine Learning) und bezieht sich auf den Bereich der künstlichen Intelligenz (KI), in dem Computer Algorithmen und statistische Modelle verwendet, um **aus Daten zu lernen und Vorhersagen oder Entscheidungen** zu **treffen**.
- **DL** steht für **Deep Learning** und ist eine Teilmenge des maschinellen Lernens, die sich auf künstliche neuronale Netzwerke konzentriert. **Deep Learning ermöglicht es Computern**, **komplexe Muster und Strukturen** in den Daten zu **erkennen** und hochentwickelte Aufgaben wie **Bild- und Spracherkennung durchzuführen**.
- **GenAI** steht für Generative AI (z.B. ChatGPT, OpenAI) diese verwendet Algorithmen, die neue Inhalte erzeugen können – sei es Text, Bilder oder sogar Code – basierend auf gelernten Mustern und Daten.
- **NLP** – NLP steht für Natürliche Sprachverarbeitung (engl. **Natural Language Processing**), die es Maschinen ermöglicht, menschliche Sprache zu verstehen, zu interpretieren und z. B. Anweisungen umzusetzen.

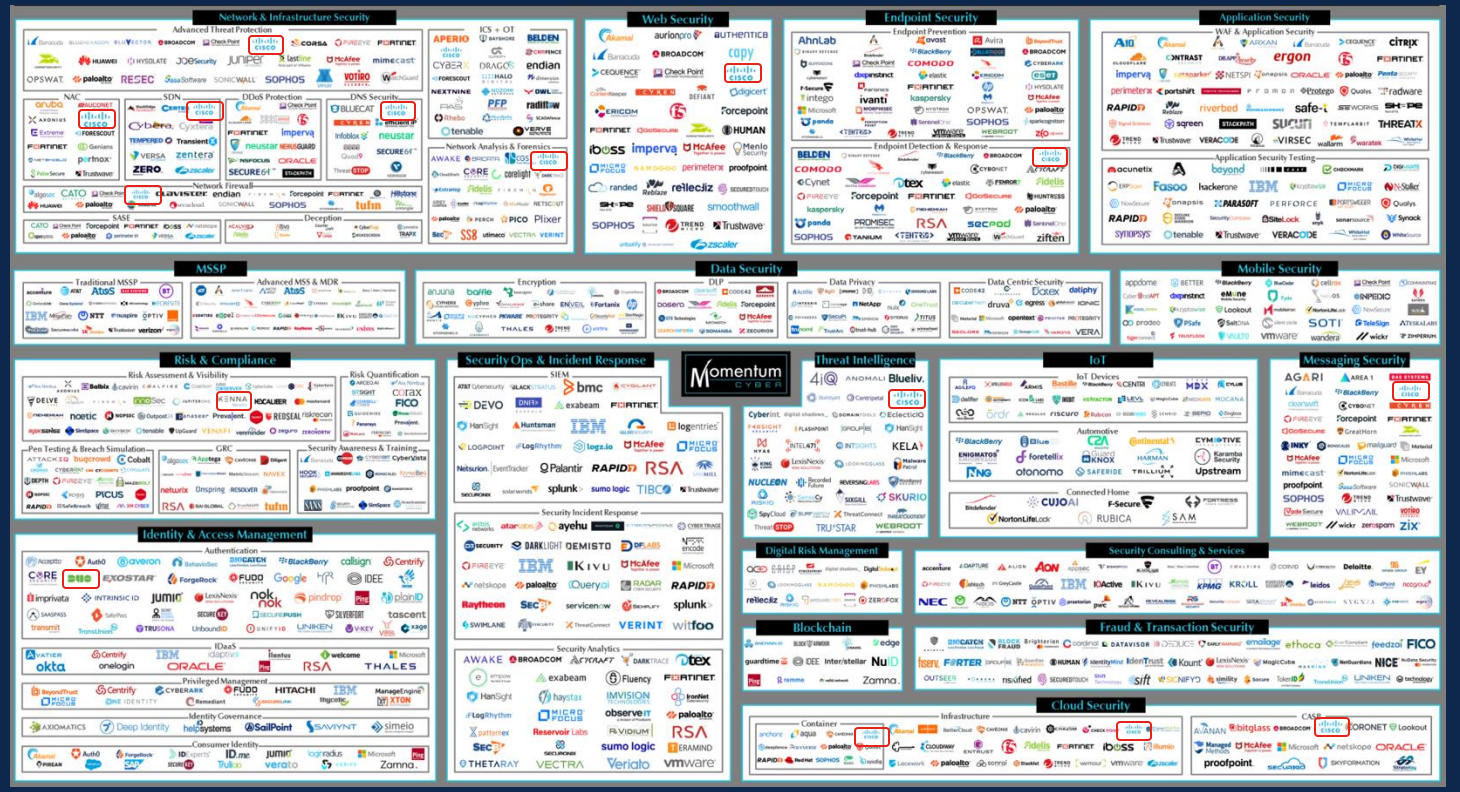


Source: https://datasolut.com/machine-learning-vs-deep-learning/

Die Herausforderung ...

- **Komplexere Netze**
  Unterschiedliche Technologien/mehr Standorte

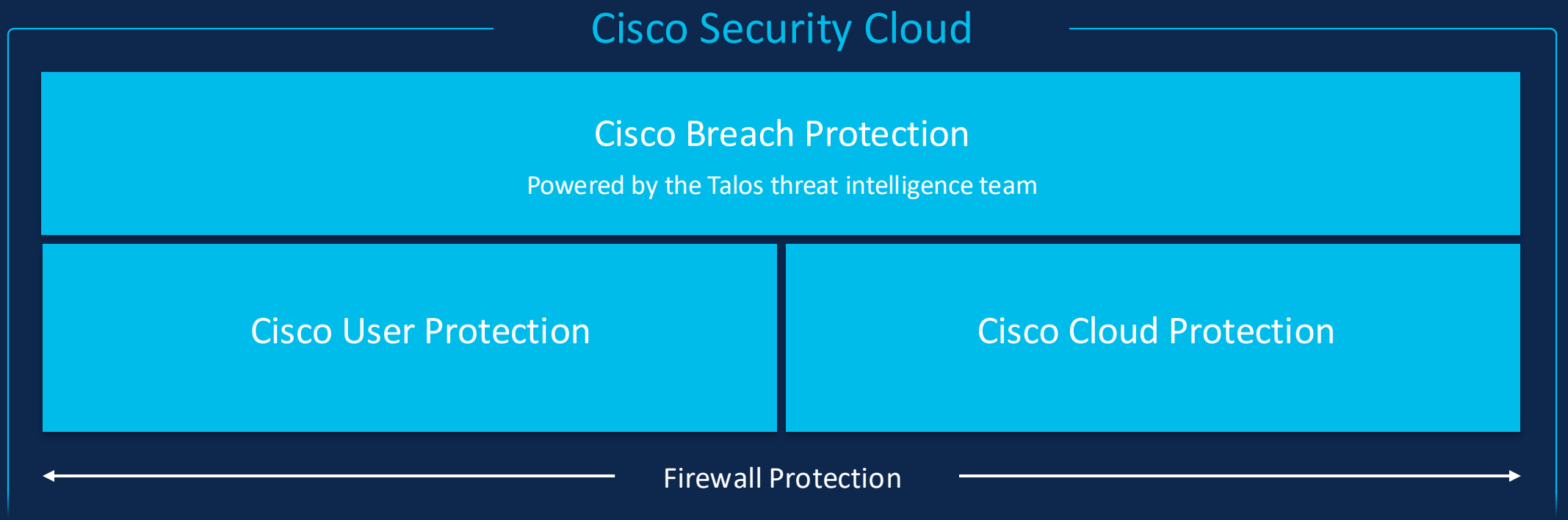
Ein Hersteller Buffet ist keine Strategie!



Unsere Kunden brauchen ein Ökosystem statt fragmentierter Lösungen !!!

Cisco Cyber Security Eco System

“If it´s connected, you´re protected”



Cisco Security Cloud

Cisco Breach Protection

- Extended Detection & Response

Cisco User Protection

- Posture & Auth Management
- Endpoint Security
- Email Security
- Experience Insights
- Remote Browser Isolation
- Network Access Control
- Security Service Edge

Cisco Cloud Protection

- Workload Security
- Application Security
- Vulnerability Management
- Full Stack Observability
- Multicloud Defense

Firewall Protection

Wir integrieren KI in das gesamte Sicherheitsportfolio

Cisco Secure AI-Assistant

Unterstützen

KI-Assistenten

Verleihen Sie Ihren Admins „Superkräfte“. Vereinfachen Sie das Management, verbessern Sie die Ergebnisse.

Augmentieren

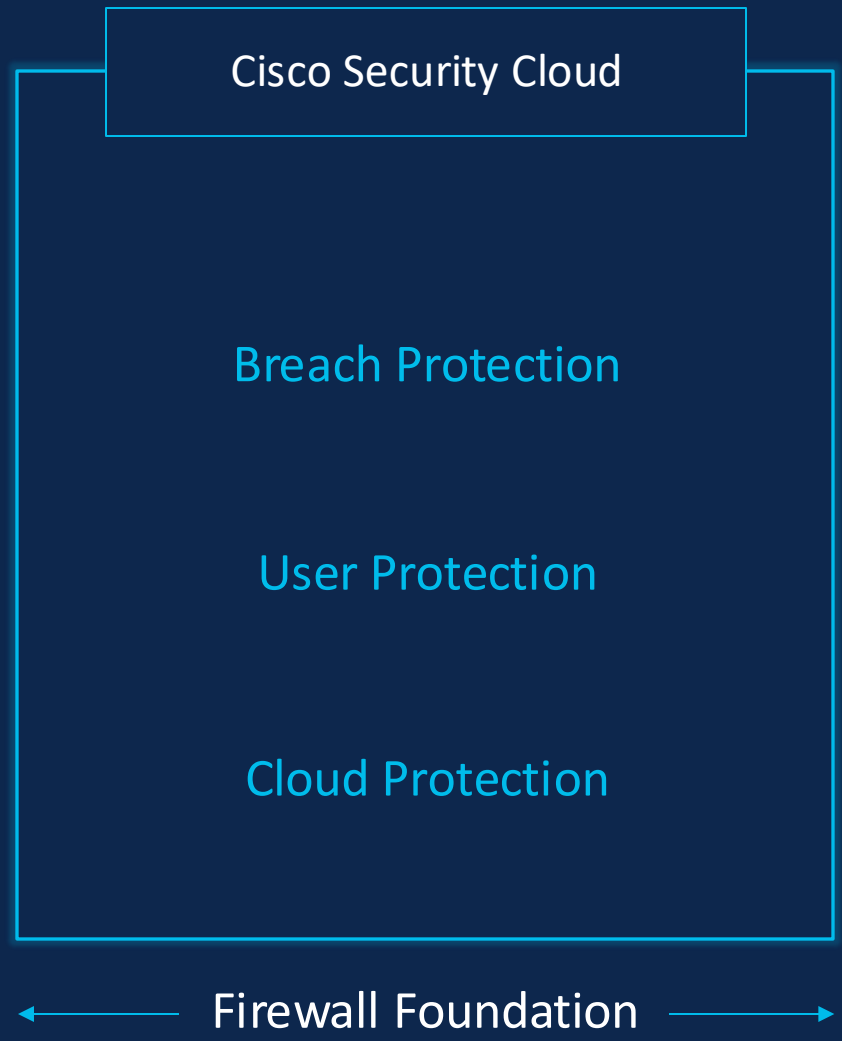
KI-gestützte Erkennung

Korrelieren Sie 550 B Sicherheitsereignisse mit Maschinengeschwindigkeit.

Automatisieren

Autonome Aktionen

Lernen Sie aus Interaktionen zwischen Mensch und Maschine, um komplexe Playbooks zu automatisieren.



KI-Assistent in der Firewall

Beschleunigen Sie Richtlinienabfragen, Problembehandlung und Regelverwaltung

Identifizierung und Berichterstattung von Richtlinien

Konfigurationsinformationen mit einem Klick

Problembehandlung und Bedrohungsabwehr

Korrelieren Sie Dokumentation und Erkenntnisse mit Maschinengeschwindigkeit

Verwaltung des Richtlinienlebenszyklus

Ergreifen Sie Maßnahmen, um neue Regeln zu erstellen oder bestehende zu blockieren

Vereinfachung der Verwaltung von Firewall-Richtlinien

2024 Forrester® Waveを for Enterprise Firewall Solutions

"Cisco advances its Secure Firewall ***into the future with innovation and a strong vision.****"*

"Cisco's vision aligns well with its networking strengths, ***leveraging these strengths to craft a security strategy that envisions the seamless integration of AI and security in the networking fabric.****"*

"Cisco distinguishes itself with a multilayered approach to traffic inspection and decryption."

Cisco Secure Firewall Appliance Portfolio

(Approximate Datasheet AVC+IPS Throughput figures)

NEW

3-6 Gbps

1200C

<1 Gbps

1010

2-5 Gbps

1100 Series

2.5-10 Gbps

2100 Series

10-45 Gbps

(Cluster up to 8)

3100 Series

65-145 Gbps

(Cluster up to 16)

4200 Series

2.5-10 Gbps

4100 Series

9300

Branch

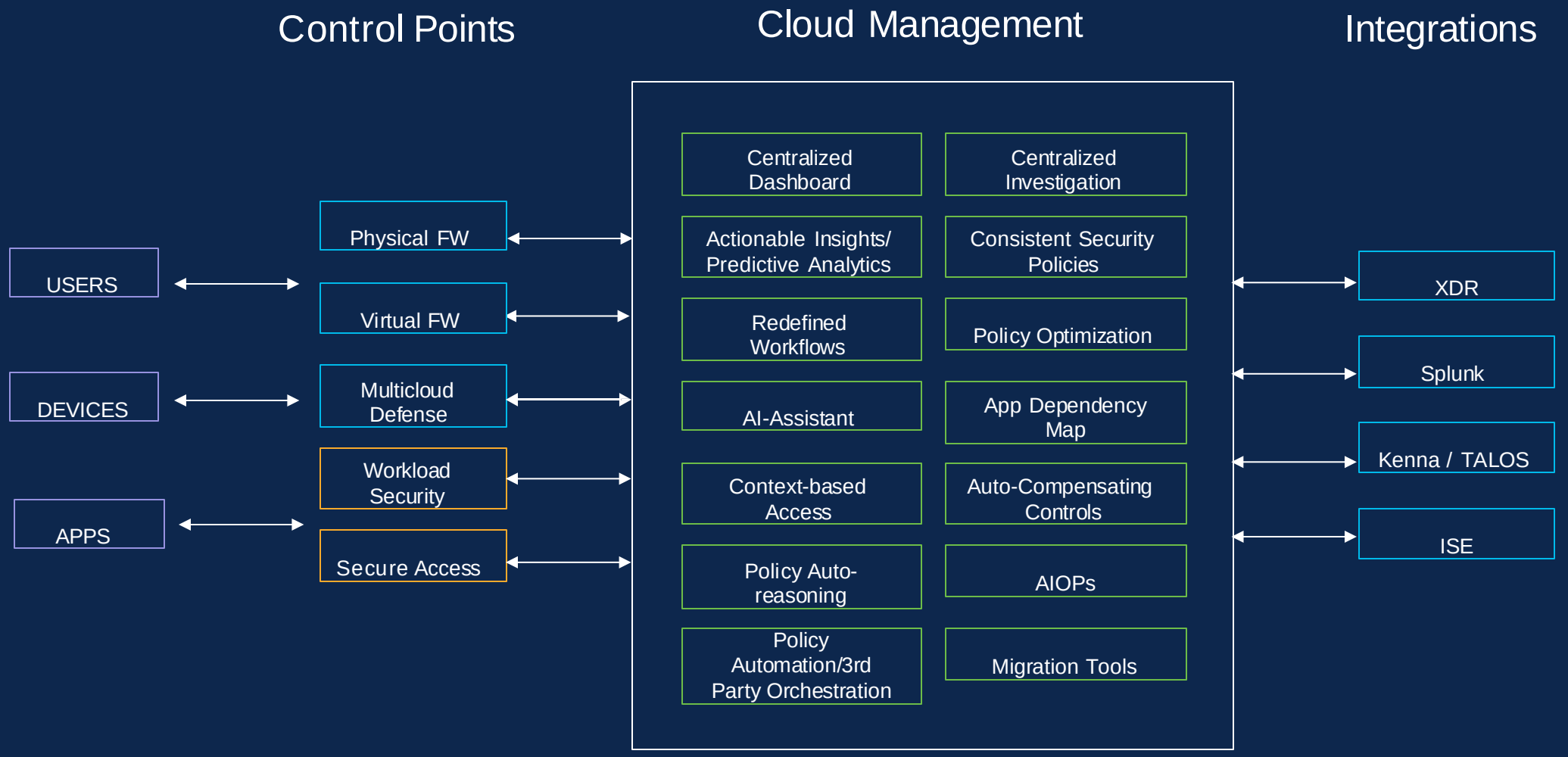
Campus

Data Center

Service Provider

SECURE

CDO Completes the Vision



Multi Tenant with Consistent API's, Identity, Context, Threat Intel, and Access

Roadmap

Preview/GA: June 2024

- AI Assistant
- Cloud On-ramp, Object Share
- AIOps for Firewall
- Kenna Integration

cisco SECURE

Cisco Secure Firewall or Cisco Meraki MX?

What does your customer value most?

Cisco Secure Firewall

On-premises management with granular controls

Customizable threat defense with deep visibility

Firewall clustering and multi-instances

Extensive integration options

Cisco Meraki MX

Cloud platform for SD-Branch management and configuration

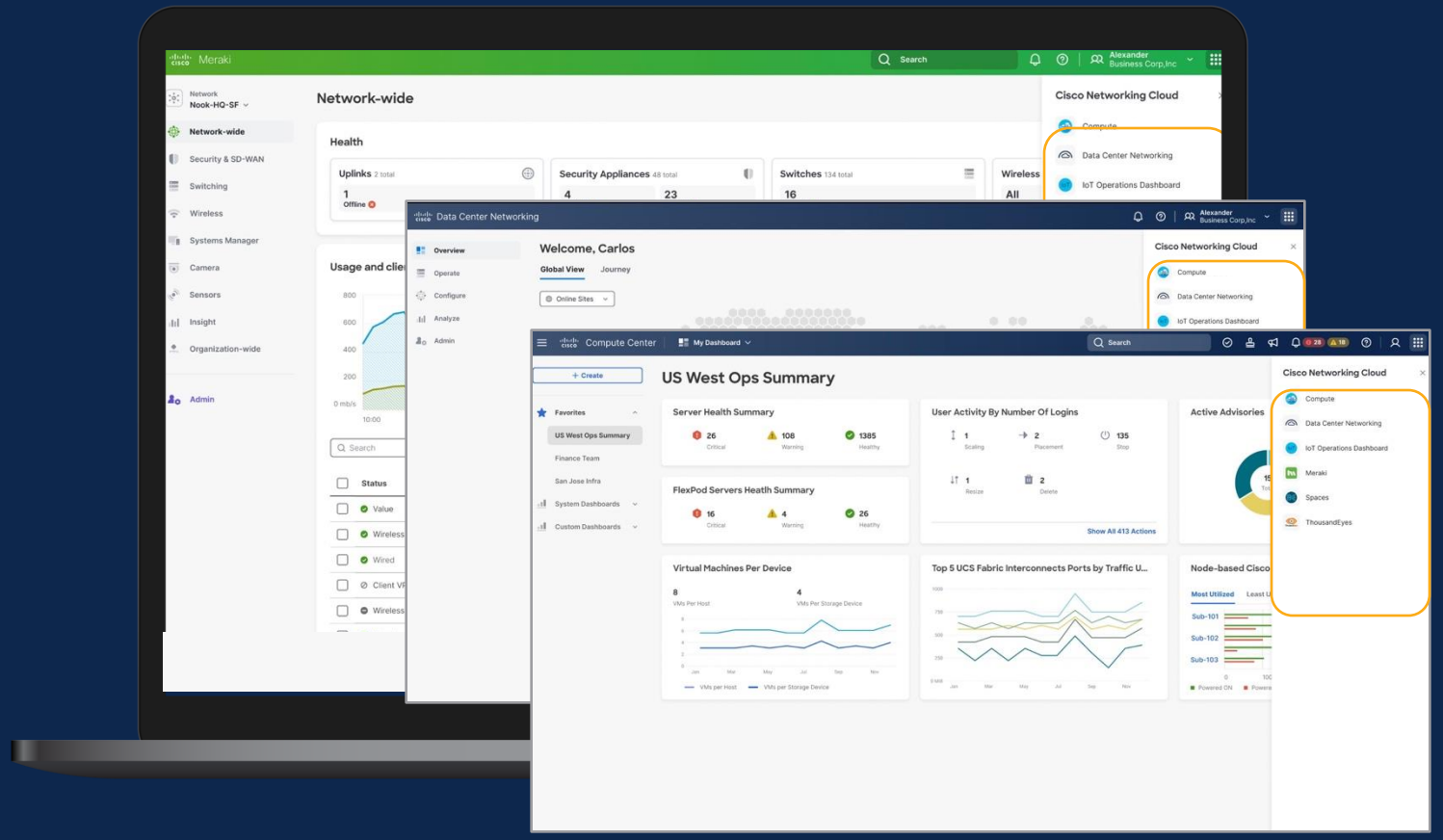
All-in-one NGFW, Cisco Secure Endpoint, IDS/IPS, and content filtering

Cloud security integration with Cisco Umbrella

Zero-touch Talos security updates

Vereinfachung

- Single Sign-On
- Einfach zwischen Anwendungen wechseln
- Optimiertes Management
- Einheitliches Designsystem

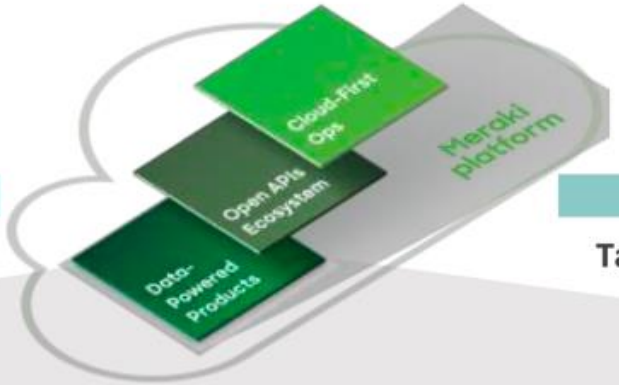


Meraki *Launchpad* for a Cisco Platform

3x larger than competitors

MERAKI DASHBOARD

Built-in solutions



API

Tailored solutions

CUSTOM BUILT

developer.cisco.com/meraki

TECH PARTNERS

meraki.com/marketplace

Wireless

Switching

Mobile Device Management

Security and SD-WAN

Cellular Gateways

Smart Cameras

Sensors

ACCESS

SECURITY AND IOT

Cisco Umbrella

Cisco ISE

Cisco AMP

Cisco DNA Spaces

Cisco AnyConnect

Cisco SNORT IDS/IPS

Cisco Stealthwatch

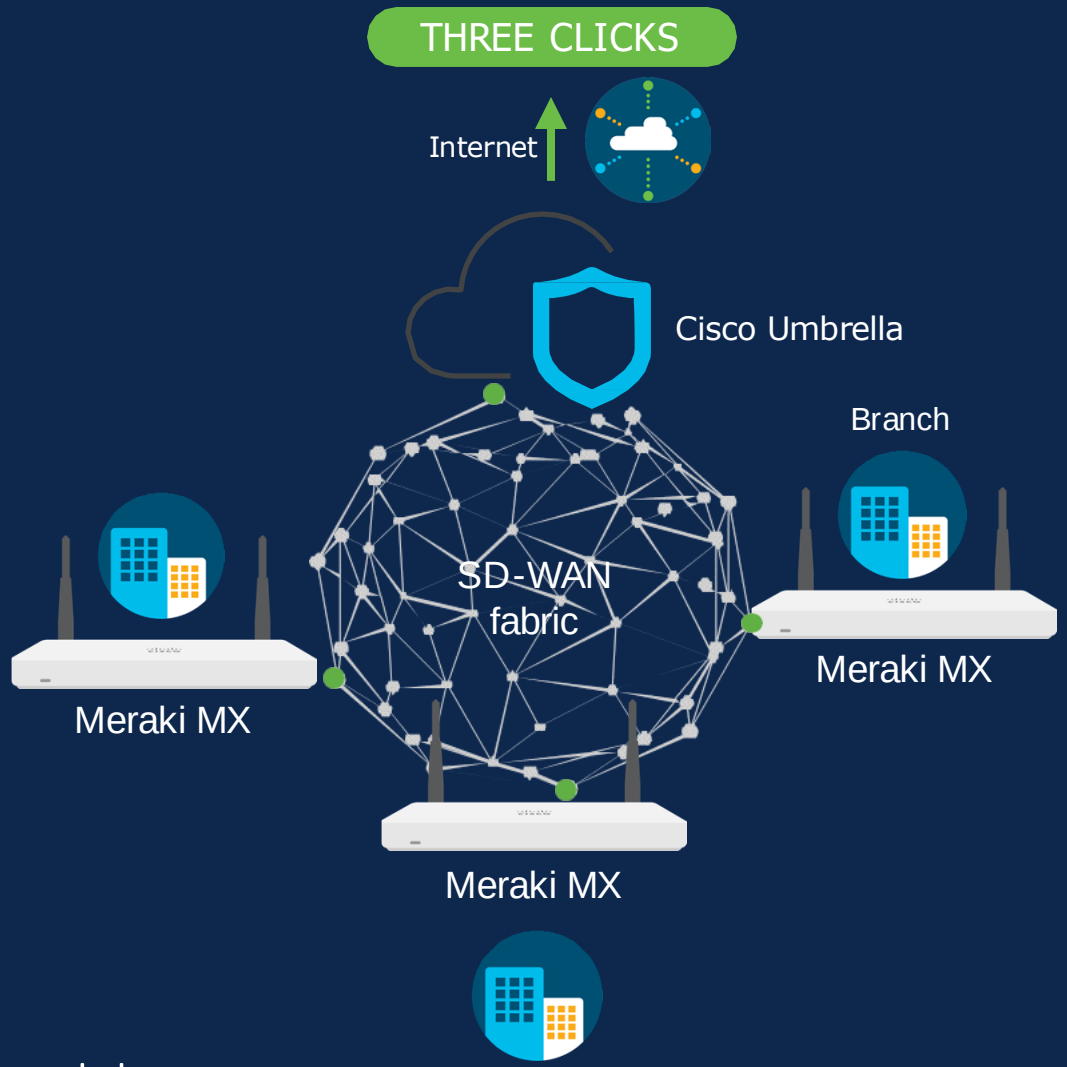
Cisco Duo

ThousandEyes

Cisco DNA

Cisco Enterprise Agreement

Supreme simplicity



Supreme security

BEST-IN-CLASS

- ✓ Layer 7 firewall
- ✓ IDS/IPS
- ✓ Content filtering
- ✓ Malware protection
- ✓ Sandboxing
- ✓ AnyConnect remote VPN access
- ✓ Centralized enforcement, policy & reporting
- ✓ Site-to-site Auto VPN
- ✓ East-west security filtering
- ✓ URL filtering
- ✓ SSL decryption/inspection
- ✓ Data loss prevention (DLP)
- ✓ Remote browser isolation (RBI)
- ✓ Granular app control
- ✓ File type control
- ✓ SaaS tenant restrictions
- ✓ CASB

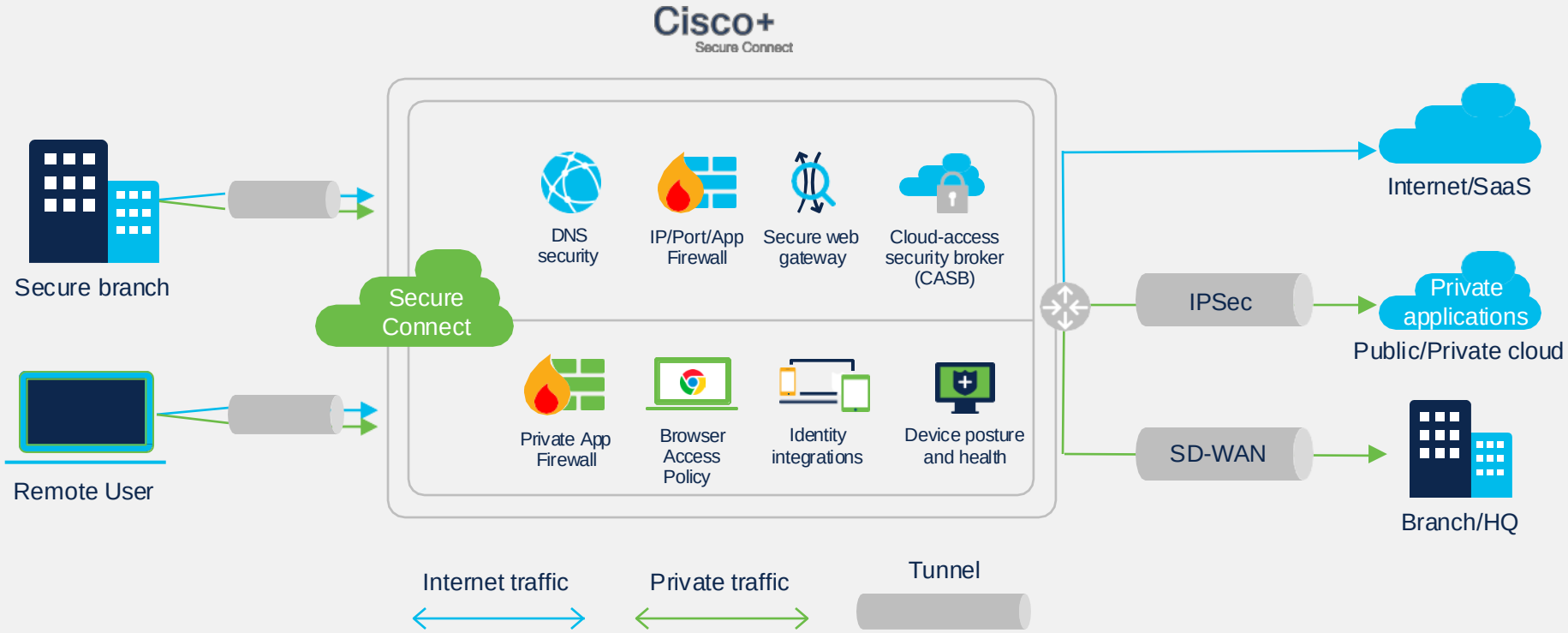
cisco SECURE

Cisco+ Secure Connect

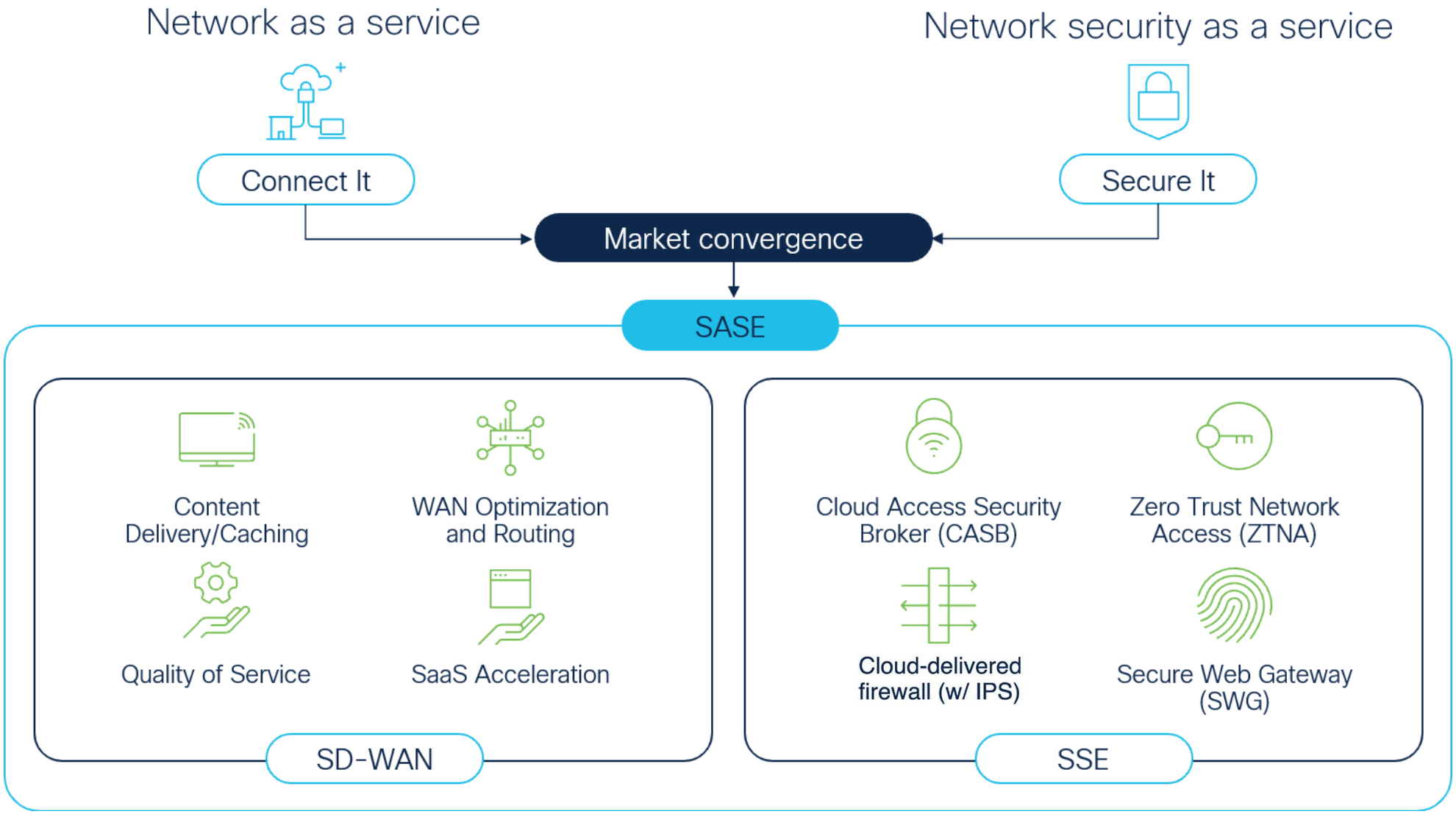
Einheitliche Sicherheitsfunktionen

Core elements

- Secure Internet and SaaS Controls (Umbrella SIG)
- Unified Private Application Access Policies
- Client and Clientless Private App Access
- Native Device posture and health support
- IDP Integrations

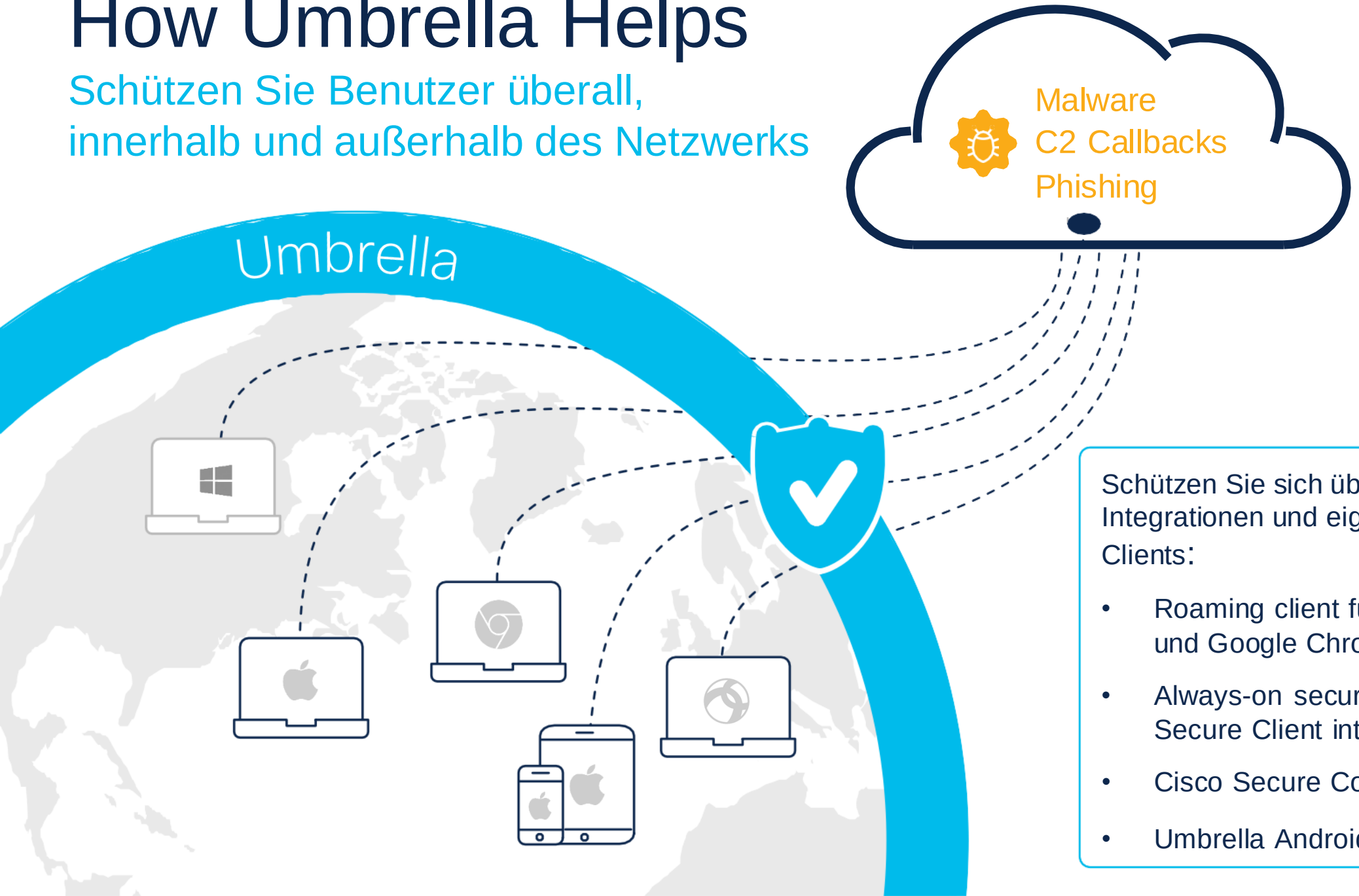


What is Secure Access Service Edge (SASE?)



How Umbrella Helps

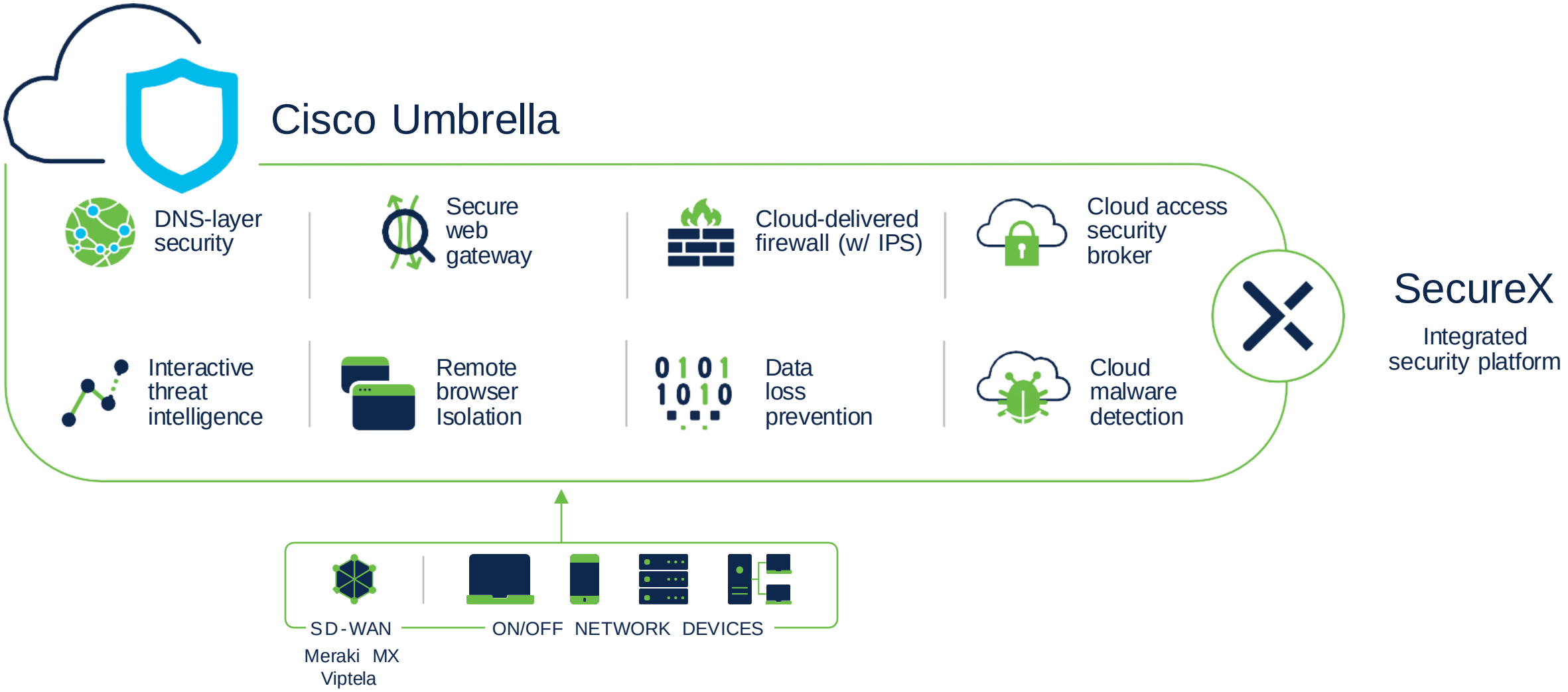
Schützen Sie Benutzer überall, innerhalb und außerhalb des Netzwerks



Schützen Sie sich überall mit Integrationen und eigenständigen Clients:

- Roaming client für Windows, Mac, und Google Chromebook
- Always-on security mit Cisco Secure Client integration
- Cisco Secure Connector für iOS app
- Umbrella Android client

How Umbrella Helps



Warum Cisco ?

Unübertroffener Überblick über die gesamte Bedrohungslandschaft

Weltweit grösstes „Threat Reseach Team“ mit über 500 Personen

550 Mrd. Sicherheitsereignisse pro Tag

~9 Mio. E-Mails blockiert pro Stunde

~2.000 neue Proben pro Minute

~2.000 blockierte Domains pro Sekunde

New Security GTM Incentives & Promotions

Early JUNE Launch

Customer Assessment Incentive

Incentivize partners to complete customer assessments resulting in security deal registration

Firewall Upgrade Incentive

Pay partners as they upgrade customer Firewall software to unlock latest features

LIVE NOW!

Targeted Competitive Firewall

Combat competitive pressures in firewall via aggressive discount

Suites Protection & Ramp

Alleviates displacement costs when migrating to Security suites via ramp credits

Concierge Deal Support

Accelerates registered security deals for partners by finding the resources to win

The bridge to possible