TD SYNNEX

Da MPLS a SASE con la soluzione Prisma

La migrazione delle reti geografiche secondo Palo Alto Networks

31 Ottobre 2025

Webinar

Riccardo Tesi – Sales Specialist – TD SYNNEX
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

TD SYNNEX

Cyber Security Awareness Month

Why Palo Alto Networks? Innovation Built for Your Security Journey

Data

Each day we analyze

1.4B+

new and unique objects across network, endpoint and cloud

R&D Investments

Invested nearly

$1.7B+

In research per year

Growth

Acquired

19

Companies in 10 years to protect customers

Efficacy

Leader in

22

Magic Quadrants and Waves

Why Palo Alto Networks?

Recognition

90

Of Fortune 100
rely on
Palo Alto Networks

Leader

#1

In Enterprise Security
by revenue size

Growth

95K

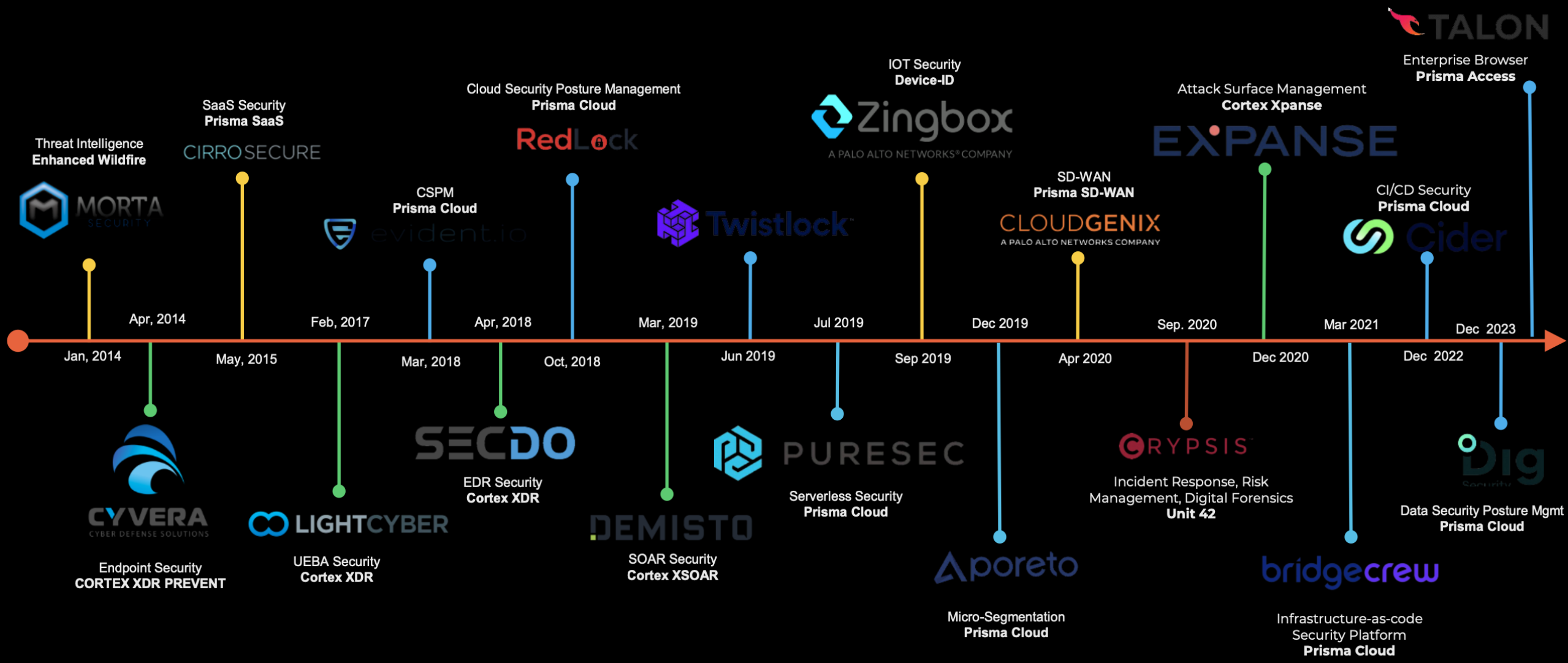
Customer Globally
in 150 Cuntries

Efficacy

15K+

Employees
globally

Acquisition



paloalto NETWORKS

NextWave Solution Provider Path | Levels

Entry level with the ability to specialize

Recognized for having **focused expertise** with PANW products & services

Recognized for having **broad expertise** with PANW products & services

Highest level and recognized for having the **broadest expertise** with PANW products & services

Limited *Breadth of Palo Alto Networks Portfolio Expertise* ***Extensive***

Solution Provider Path | Requirements

	Registered[1]	Innovator	Platinum Innovator	Diamond Innovator
Performance	**Total Bookings or Deal Reg Pipeline**	**Total Bookings or Deal Reg Pipeline**	**Total Bookings or Deal Reg Pipeline**	**Total Bookings or Deal Reg Pipeline**
Country Set A1	--	$200K or $600K	$5M or $15M	$15M or $30M
Country Set A		$100K or $200K	$1.5M or $4.5M	$5M or $15M
Country Set B		$50K or $100K	$1M or $3M	$3M or $9M
Country Set C		$20K or $40K	$500K or $1.5M	$1.5M or $4.5M
Capabilities & Engagement				
Sales	--	1 Product Specialization	2 Product Specializations	3 Product Specializations
Technical Pre-Sales				
Certified Full-Time Engineers	--	--	At least **3 FTEs each with minimum 1 advanced technical cert[2]** in corresponding specializations	At least **4 FTEs each with minimum 1 advanced technical cert[2]** in corresponding specializations
Business Requirements				
NextWave Solution Provider Agreement & Foreign Corrupt Practices Act	✓	✓	✓	✓

Note: Chart in US dollars | [1]Registered partners in the program for 2 years with $0 bookings & $0 pipeline will be removed | [2]Eligible advanced technical certs include those listed in the FTE Requirements Table

NextWave Product Specializations

	Sales	Technical Sales Readiness	NextWave Certification
Hardware Firewall	SPS HW Firewall	Hardware Firewall	Network Security Professional
Software Firewall	SPS SW Firewall	Software Firewall	
SASE	SPS SASE	SASE	
Cortex XSIAM	SPS XSIAM	Cortex XSIAM	Security Operations Professional
Cortex XDR	SPS XDR	Cortex XDR	
Cortex XSOAR	SPS XSOAR	Cortex XSOAR	
Prisma Cloud	Prisma Cloud Cortex Cloud	Prisma Cloud Cortex Cloud	Cloud Security Professional

Product Specializations | Engagement Points

HW FW
SW FW
SASE
Cloud
XDR
XSOAR
XSIAM

- **Minimum of 20 engagement points** must be earned and maintained per product specialization in a **trailing 12-month period.**
- **Engagement points expire after one year** from the date they were earned, except for NFR points which remain valid as long as the product is active.
- **Depending on the type of activity,** engagement points may apply to some or all product specializations.
- **For more information,** refer to the Product Specialization Engagement Points Guide.

Applicable to MSSP Path only

Service Implementation Plan (SIP) = 20 points per SIP

For each new managed service offering, document the offer in a Service Implementation Plan. Then, test and validate the managed offering using the Partner Eval System (PES) or Not-for-Resale (NFR) device/license.

Product Code Version Validation (PCV) = 10 points per PCV

In subsequent years for each managed offering, update your SIP and leverage the PES or NFR device/license for testing. Finally, validate that your offering is running the current version of product code.

Beacon Tools Course = 5 points per completion

Course providing context for utilizing tools such as PES, SLR, and UTD for scaling customer sales and services.

Beacon Rules of Engagement Course = 5 points per completion

Course providing information on channel rules of engagement to help streamline your workflow with Palo Alto Networks.

Partner Eval System (PES) = 2 points per Eval

Give customers a true platform ownership experience with our comprehensive range of security subscriptions.

Security Lifecycle Review (SLR) = 2 points per SLR

Help customers and prospects gain deep visibility into applications used, network vulnerabilities, IoT devices and exposure to threats and risks.

Ultimate Test Drive (UTD) = 5 points per UTD

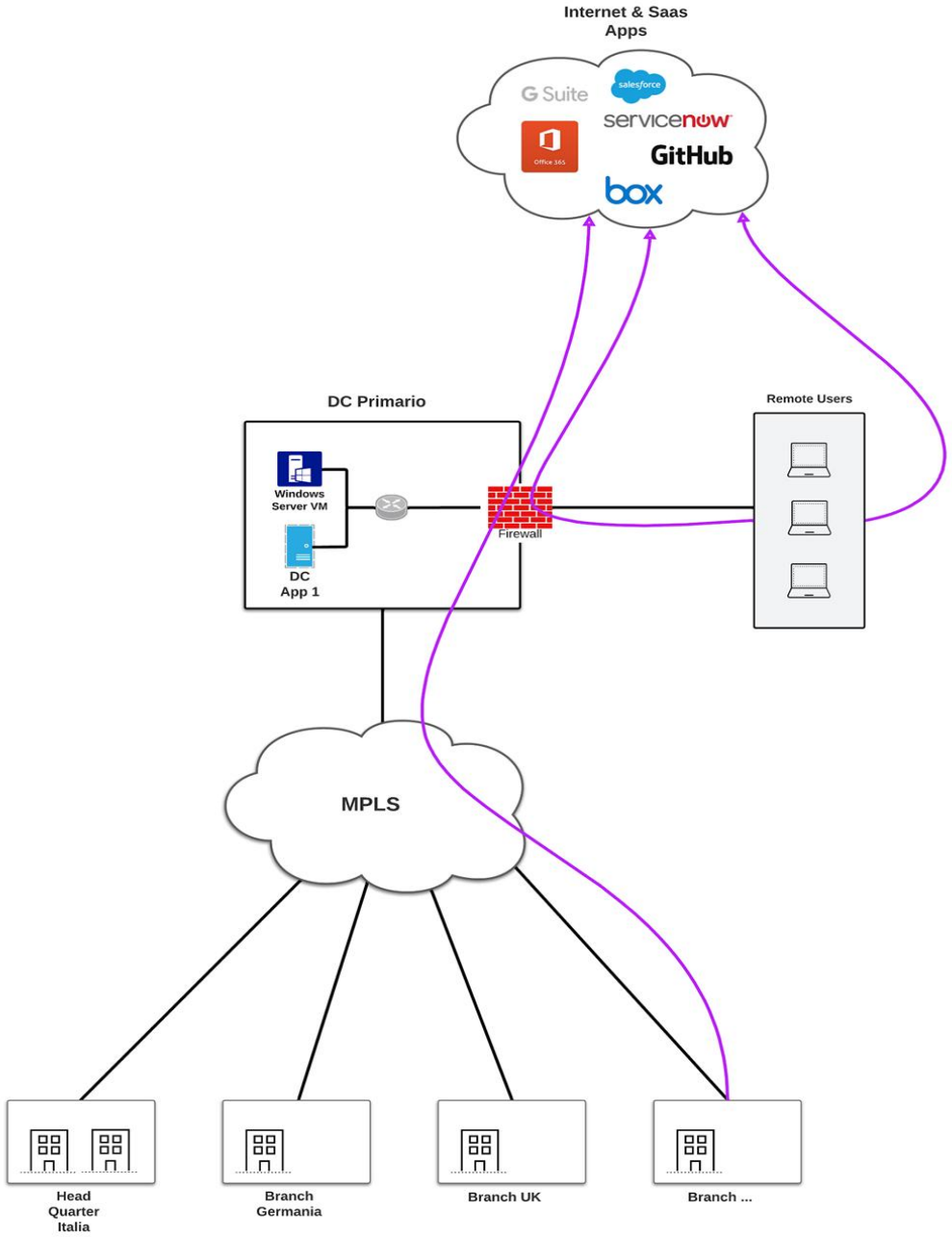
Give customers and prospects a guided hands-on experience of Palo Alto Networks' highly automated and natively integrated Security Operating Platform.

Not-for-Resale (NFR) = 1 point per device/license

Strengthen and refine your Palo Alto Networks product demo capabilities using your NFR investment.

Perché TD SYNNEX

- Presales e architettura
- Demo
- Ultimate Test Drive e SLR
- Formazione



La situazione di partenza

Azienda manifatturiera con HQ e Data Center in Italia, filiali globali e forza vendita mobile.

Architettura Tradizionale: **hub-and-spoke.**

- Tutto il traffico (filiali e VPN) è forzato verso il Data Center.
- Per motivi di performance, **il cliente ha deciso di permettere connettività diretta fra alcuni utenti remoti ed Internet/SaaS Apps sacrificando la sicurezza**.
- L'Identity è gestita da un classico Active Directory On-Prem sincronizzato con Microsoft Entra.

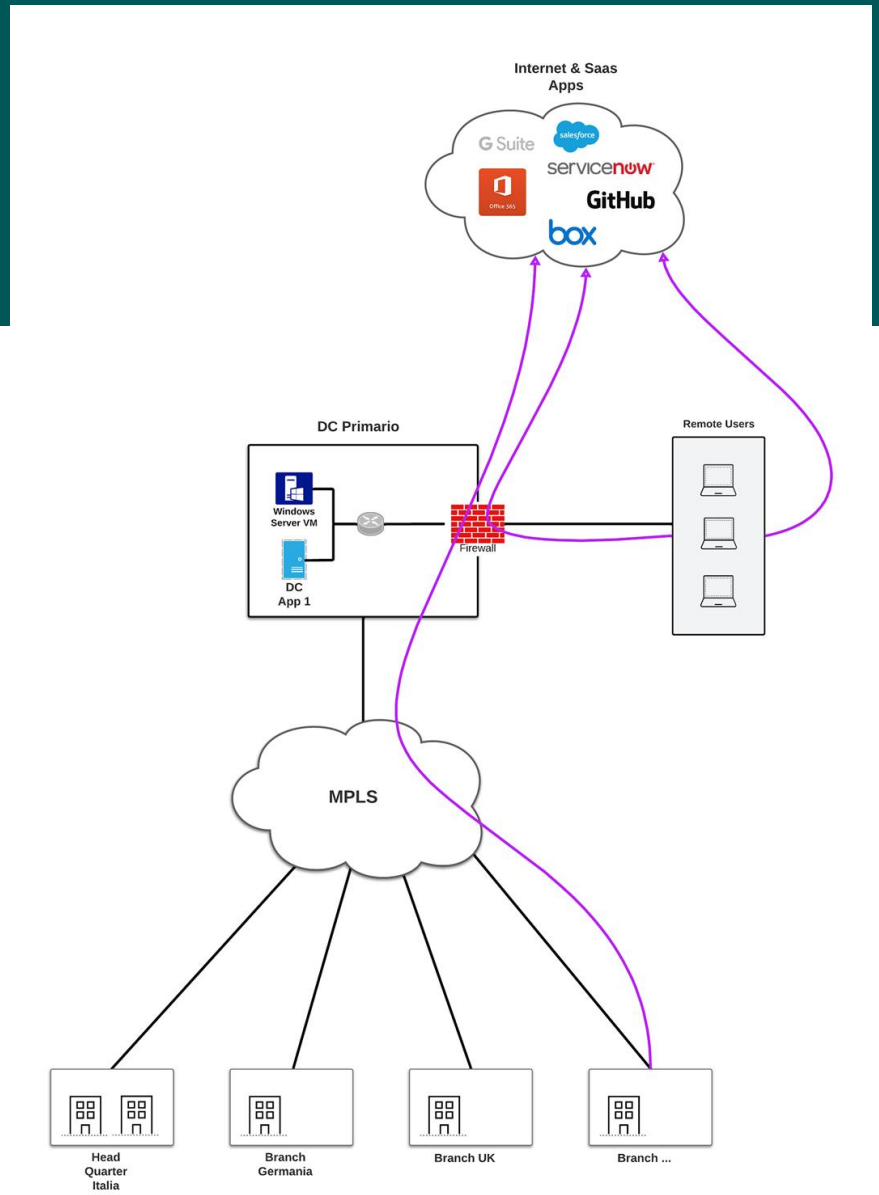
Problemi riscontrati

❌ **Esperienza utente frustrante:** Latenza elevata per le app SaaS (Office 365, Salesforce ecc).

❌ **Costi Elevati:** Dipendenza da costosi circuiti MPLS.

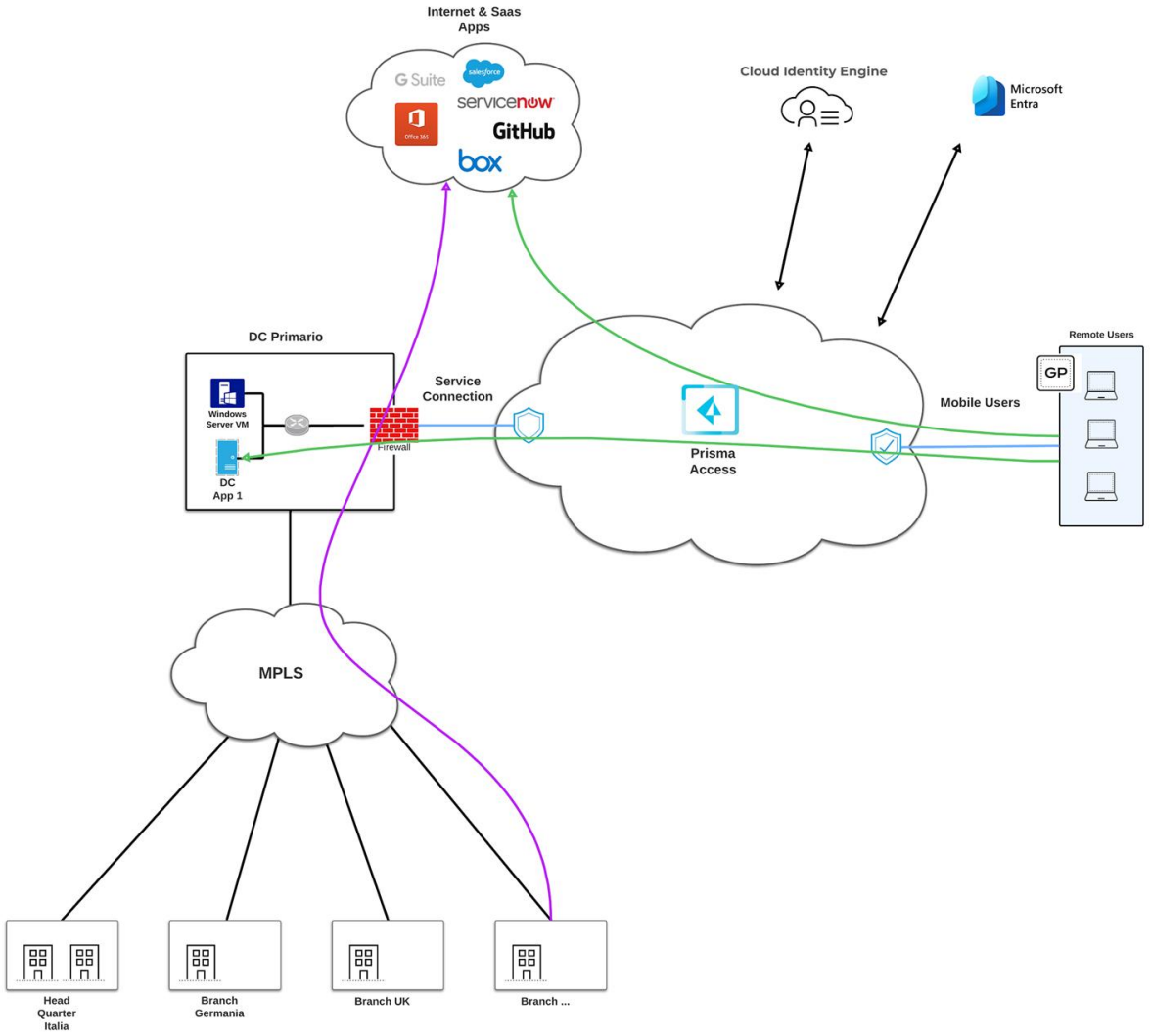
❌ **Sicurezza compromessa e complessa:** Il perimetro si è dissolto per via delle sedi ed utenti remoti, ma i controlli sono ancora centralizzati. In alcuni casi gli utenti accedono ad Internet senza ispezione del traffico.

❌ **Business rallentato:** L'apertura di una nuova filiale richiede settimane/mesi.



TD SYNNEX

1: Utenti remoti

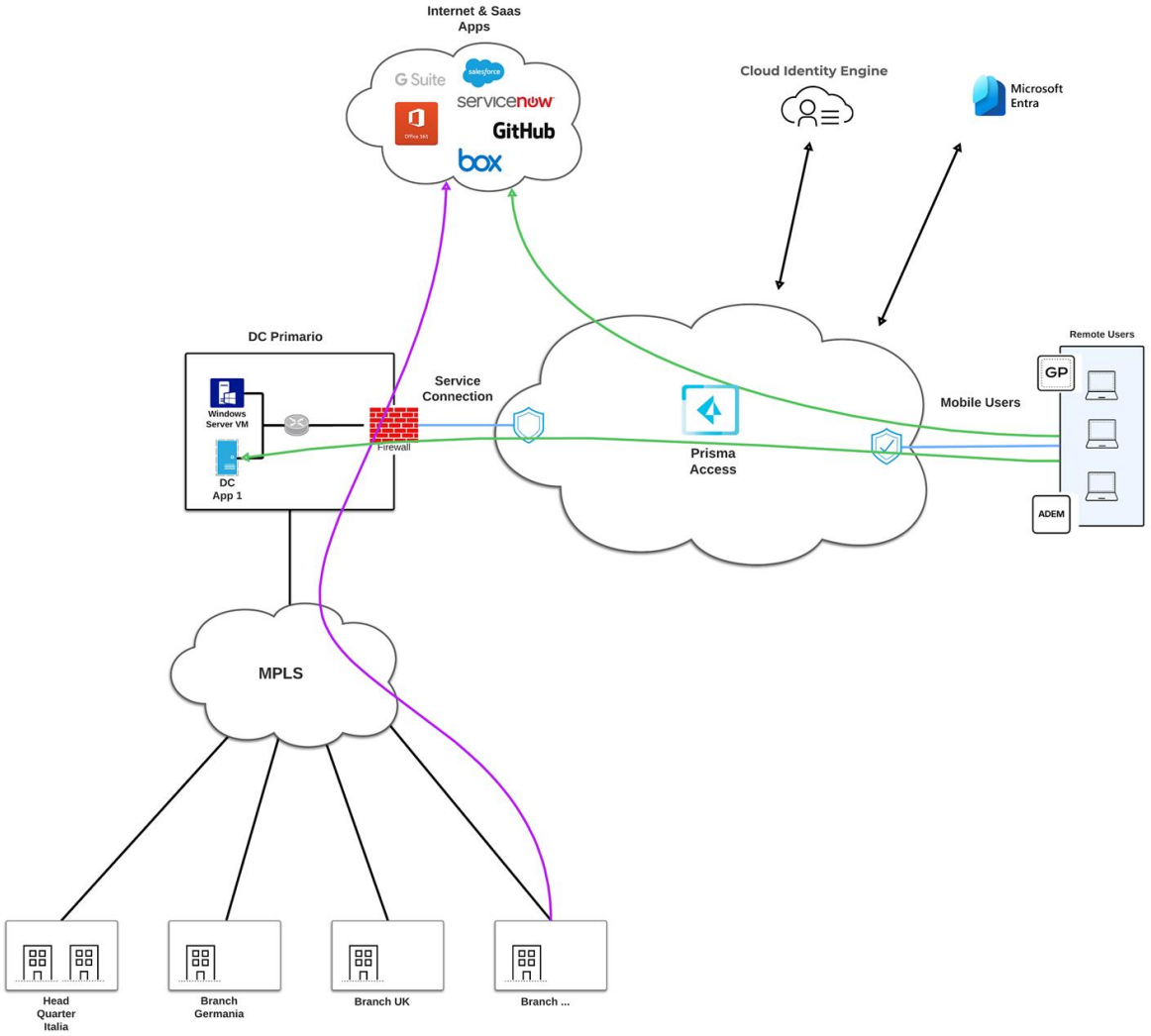


- Connessioni sempre veloci e a bassa latenza per gli utenti, ovunque si trovino nel mondo: **Best Available Gateway.**
- La stessa protezione enterprise dei NGFW contro le minacce avanzate, erogata direttamente dal cloud: **Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire**.
- Policy granulari basate su utente, dispositivo e applicazione per garantire accesso solo a chi ne ha diritto: **User-ID, App-ID, Device-ID**.

paloalto NETWORKS

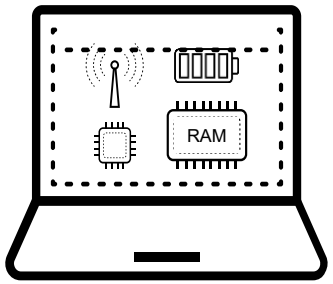
TD SYNNEX

2: Ottimizzazione - ADEM



Risolto l'accesso, il reparto IT si scontra con un nuovo problema: quando un'app è lenta, di chi è la colpa? La rete di casa? L'ISP? Prisma Access?

Per questo, nella seconda fase, attivano **ADEM**



Identifica problemi direttamente sul dispositivo dell'utente (CPU, RAM, Wi-Fi di casa) prima che apra un ticket.

Monitora l'intero percorso dal laptop all'applicazione per trovare la causa dell'anomalia

paloalto NETWORKS

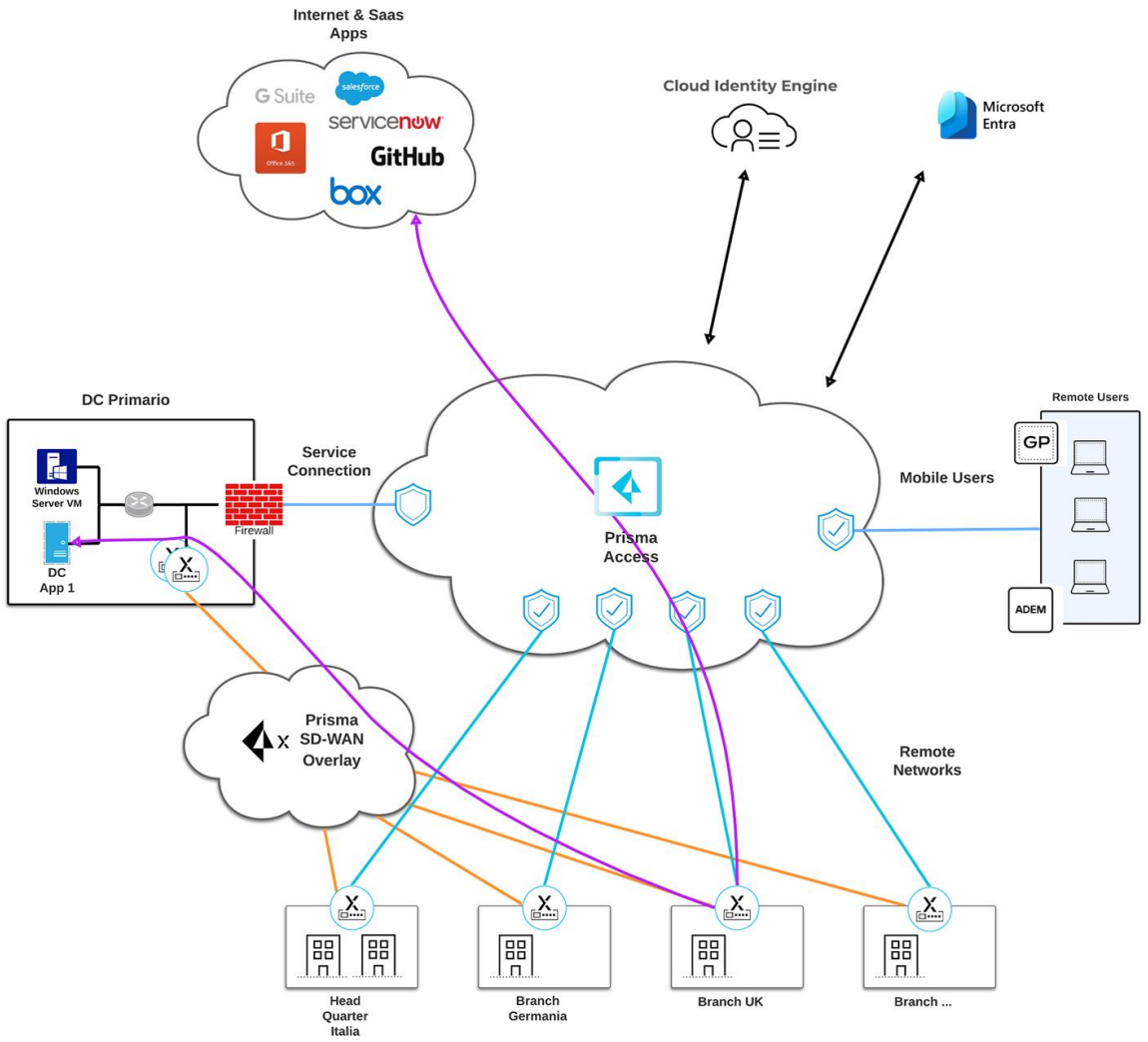
Migrazione Circuiti MPLS ad Internet

- ✓ Riduzione dei costi
- ✓ Scalabilità
- ✓ Flessibilità

- ✓ Indipendenza da ISP
- ✓ Circuiti internazionali
- ✓ Esperienza utente

TD SYNNEX

3: SASE su Branches



- **Modernizzazione della WAN**
- **Traffico Internet Sicuro**
- **Accesso Ottimizzato alle App Private**
- **Sicurezza Interna**

⚠️ Abbiamo risolto la connettività delle filiali, ma come gestiamo in modo granulare l'identità e **l'esperienza dell'utente che si trova fisicamente all'interno dell'ufficio**?

paloalto NETWORKS

4: Utenti negli uffici

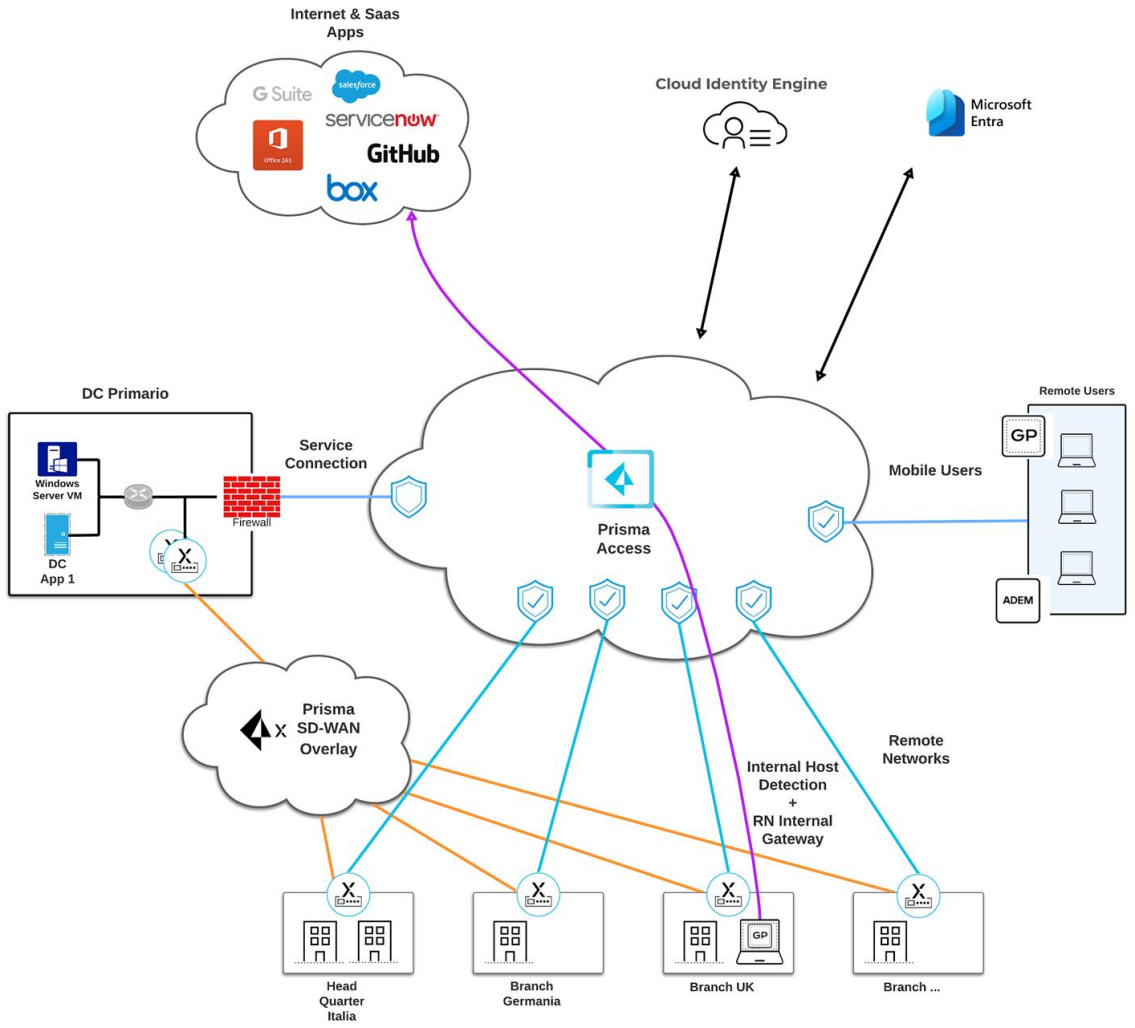
Obiettivo: Garantire un'esperienza utente trasparente e policy di sicurezza coerenti, indipendentemente da dove si trovi l'utente (a casa o in ufficio).

Da Remoto: L'agent funziona in modalità Always-On, inviando tutto il traffico a Prisma Access per la massima sicurezza.

In Ufficio: L'agent rileva la rete interna (Internal Host Detection) e disattiva il tunnel. L'autenticazione dell'utente avviene in modo trasparente, senza alcun impatto sulla sua esperienza.

Risultato per il Traffico Internet: Il gateway della filiale (Remote Network) è in grado di identificare l'utente specifico e applicare policy di sicurezza granulari basate su User-ID.

E per il Traffico Privato?

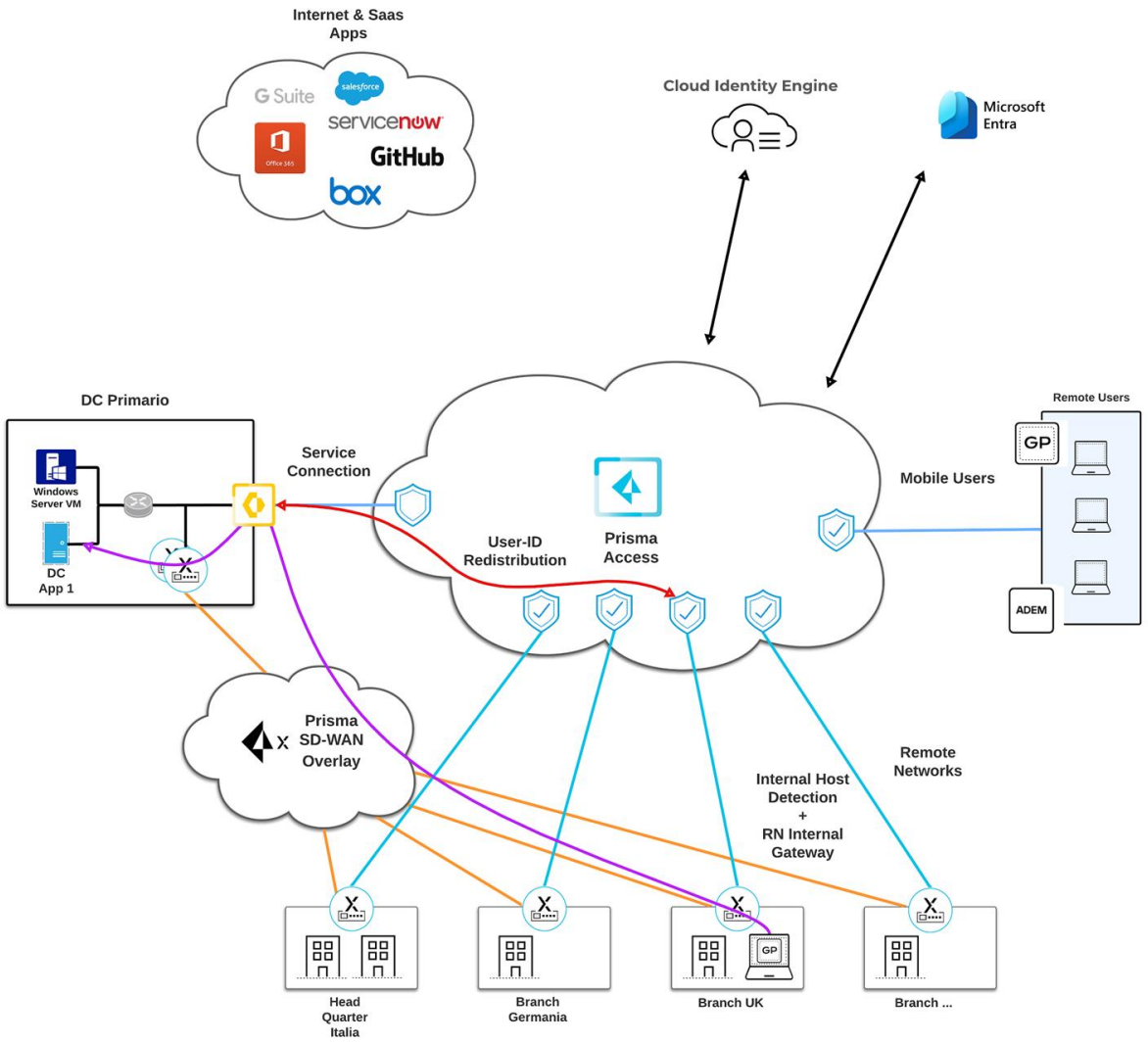


5: Ufficio verso DC

Strategia: Installiamo un NGFW come CPE della Service Connection e utilizziamo la funzionalità di User-ID Redistribution fra Remote Network e NGFW.

Risultato: Prisma Access condivide in tempo reale le informazioni di identità con il firewall del Data Center. Questo meccanismo, chiamato User-ID Redistribution, permette al NGFW on-premise di sapere esattamente quale utente sta generando traffico.

Beneficio: Coerenza Totale delle Policy. Un utente in filiale che accede a un server interno è soggetto alle stesse, identiche regole di sicurezza basate su identità che avrebbe se fosse connesso da remoto. La visibilità e il controllo sono completi, mantenendo un'esperienza utente coerente.



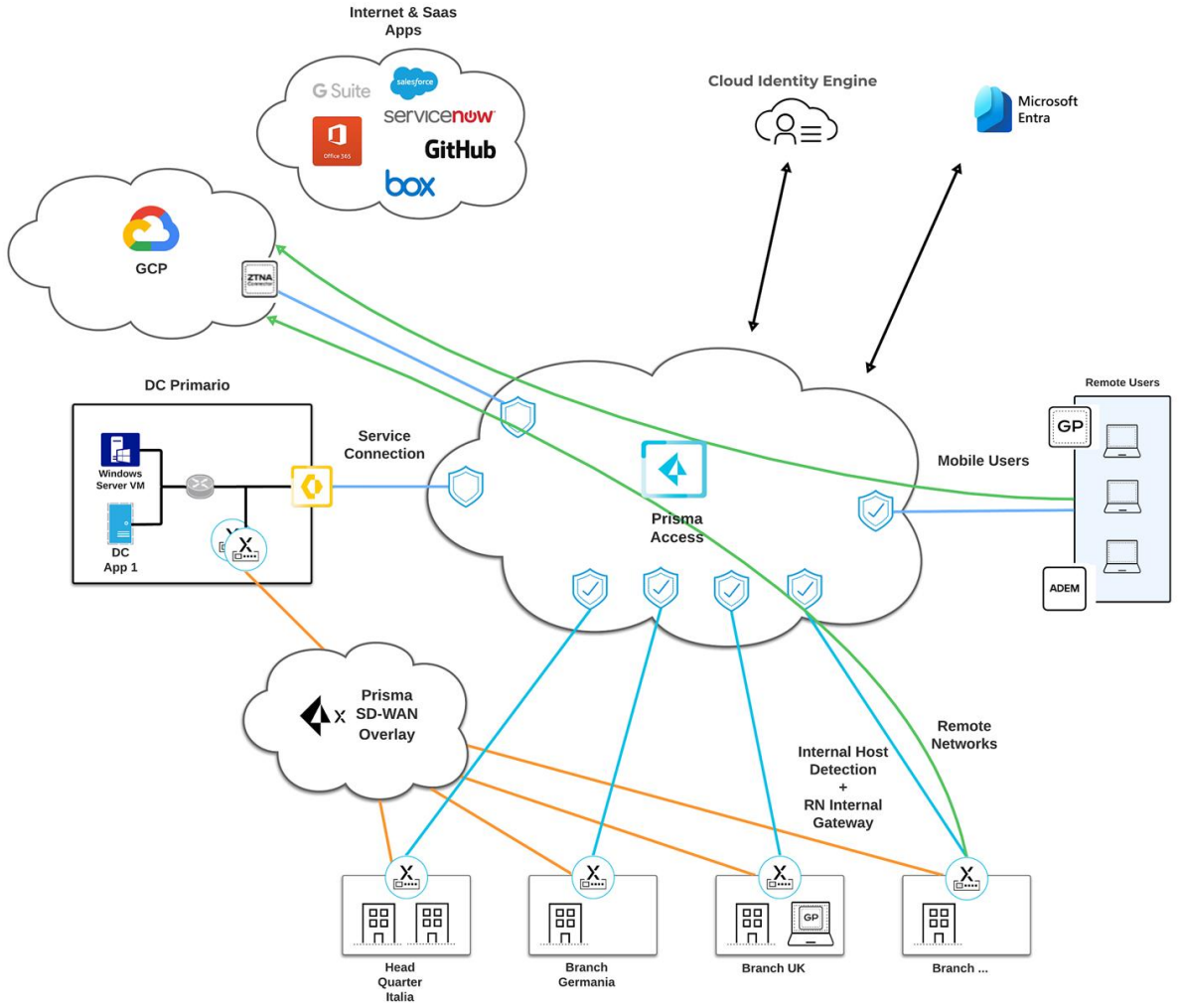
6: Connettore ZTNA

La migrazione verso il Cloud: L'azienda decide di modernizzare un'applicazione legacy, migrandola dal Data Center a un ambiente IaaS su GCP. Come possono garantire un accesso sicuro a questa risorsa senza esporla su Internet?

La Soluzione: ZTNA Connector. Viene deployato uno ZTNA Connector all'interno del VPC del cliente. Questo connettore stabilisce un tunnel sicuro e outbound verso Prisma Access.

Risultato: L'applicazione su GCP diventa una risorsa privata accessibile tramite Prisma Access, esattamente come se fosse nel DC fisico.

Gli utenti beneficiano dello stesso accesso ZTNA 2.0 sicuro e granulare, senza bisogno di configurare Tunnel VPN o applicare logiche di sicurezza in altri punti della rete.



7: Prisma Browser

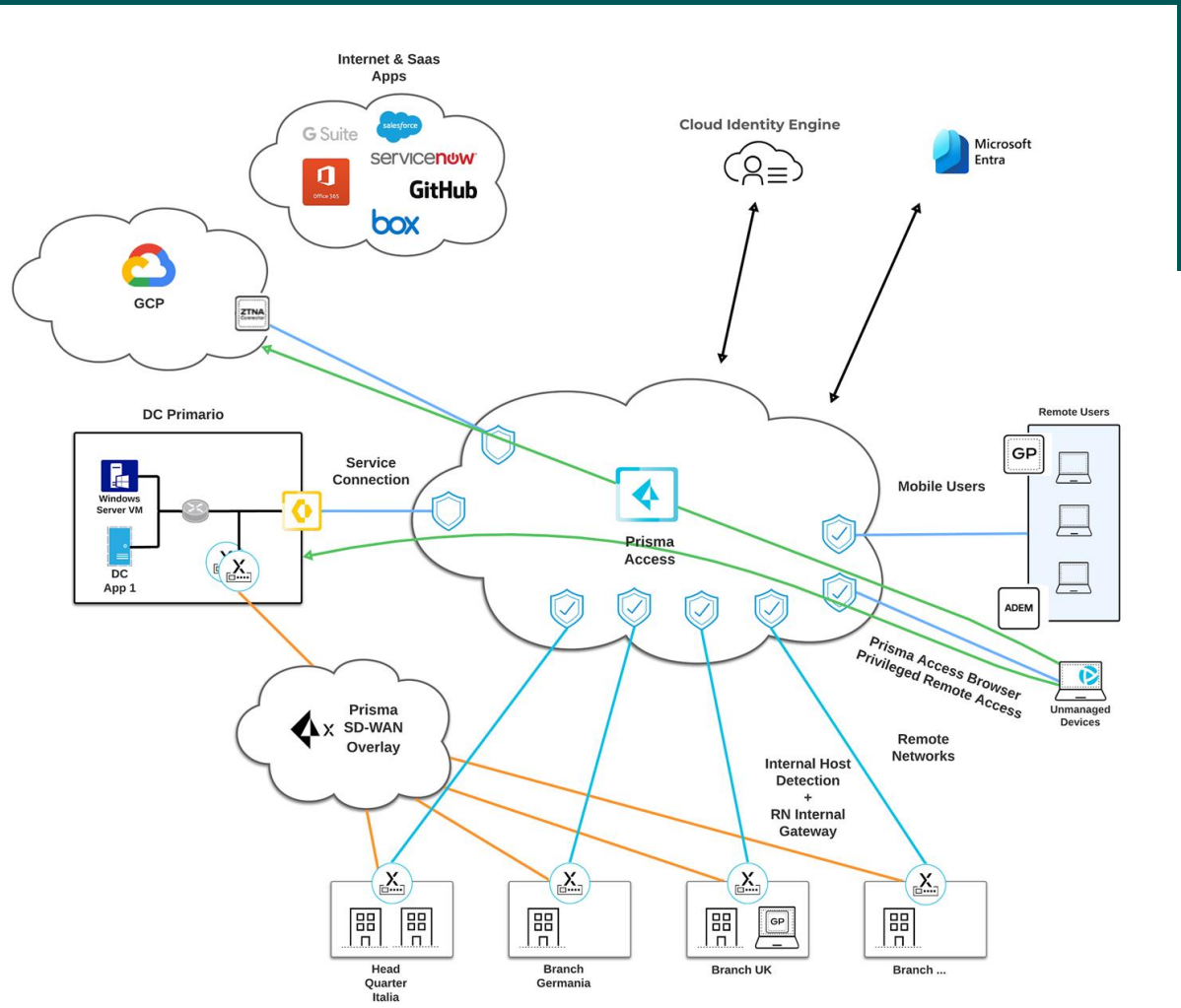
La Sfida dei Dispositivi non Gestiti: Spaghetti Systems ha bisogno di dare accesso a consulenti esterni e manutentori per interventi su server specifici. Come garantire un accesso sicuro e controllato a questi utenti che utilizzano i loro PC personali (unmanaged)?

La Soluzione: Prisma Access Browser e Privileged Remote Access.

Prisma Access Browser (PAB): Fornisce accesso ZTNA 2.0 clientless (via browser) alle applicazioni web interne.

Privileged Remote Access (PRA): Estende l'accesso clientless a protocolli non-web come SSH, RDP e VNC, registrando le sessioni per audit.

Risultato: Sicurezza Zero Trust per l'intera Supply Chain.



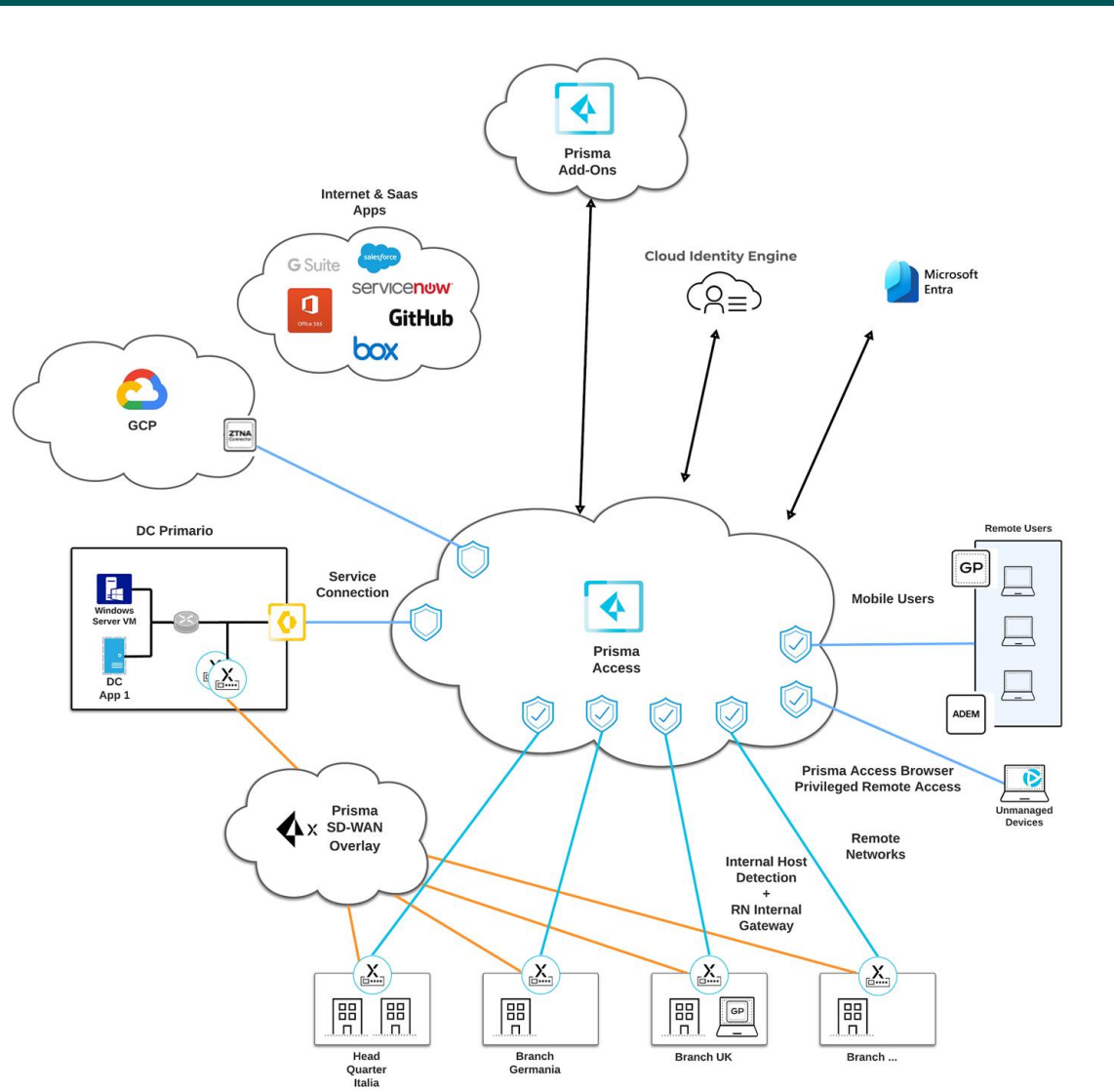
8: Implementazioni future

La piattaforma Prisma SASE è progettata per crescere con le esigenze del cliente.
Risolte le sfide di connettività e accesso, si hanno a disposizione ulteriori funzionalità

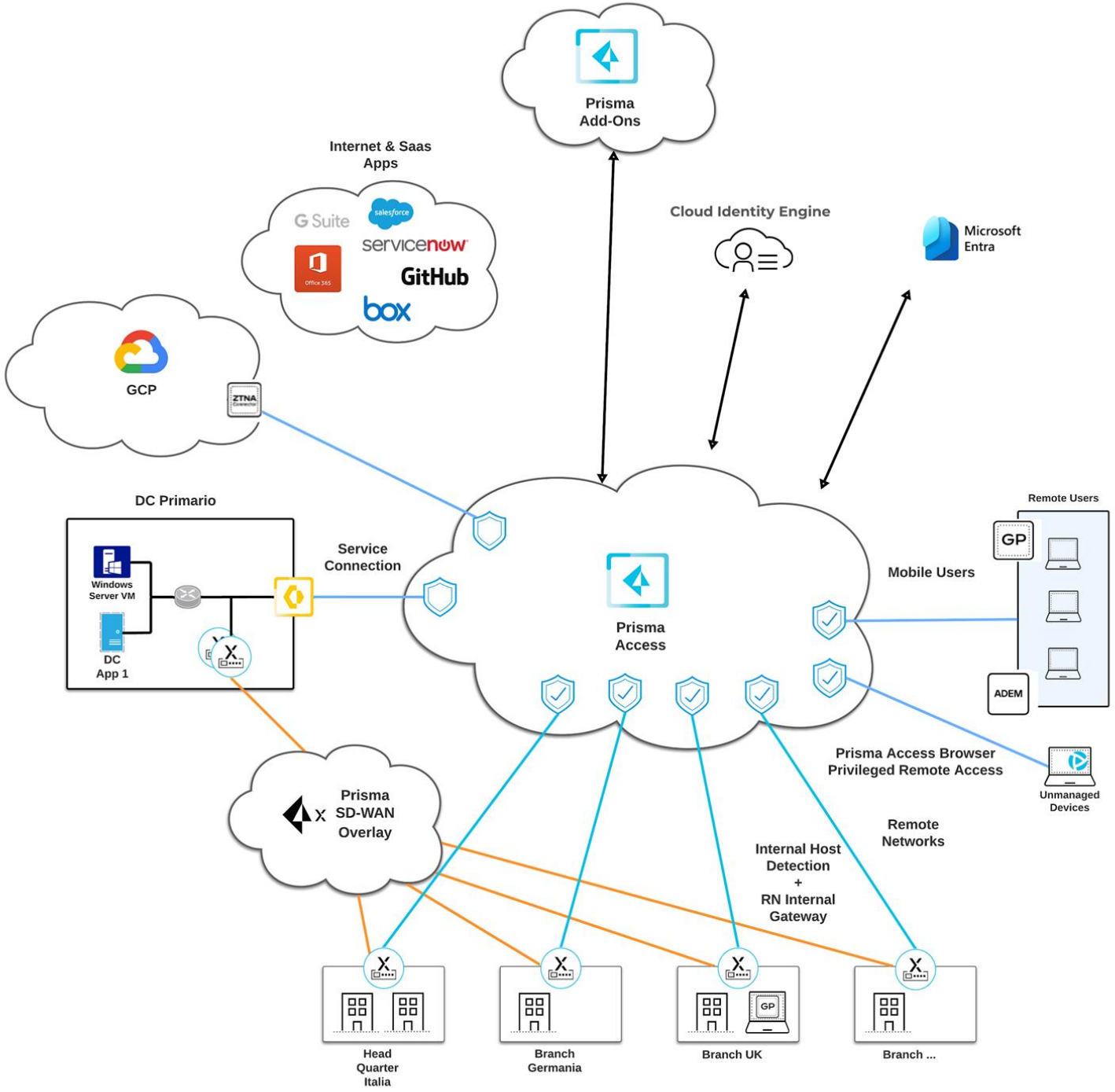
Next-Gen CASB: Per scoprire e controllare l'uso di tutte le applicazioni SaaS (anche quelle non approvate dall'IT, o "Shadow IT") o estendere il controllo ai Data-At-Rest.

Enterprise DLP: Per estendere la prevenzione della perdita di dati a tutte le app SaaS, cloud e private, con un'unica policy coerente.

RBI (Remote Browser Isolation): Per isolare la navigazione degli utenti ad alto rischio in un ambiente sicuro nel cloud.



TD SYNNEX



paloalto NETWORKS

Il risultato

Modernizzazione della WAN: Sostituzione dei costosi circuiti MPLS con una rete SD-WAN agile, intelligente e basata su connettività Internet.

Accesso Ottimizzato: Eliminazione del backhauling per il traffico Internet e accesso a bassa latenza alle applicazioni SaaS e private.

Esperienza Utente Migliorata: Produttività aumentata grazie a connessioni più veloci e a una risoluzione proattiva dei problemi tramite ADEM.

Zero Trust

Superficie d'Attacco Ridotta: Policy di accesso "least-privilege" (ZTNA 2.0) per tutti gli utenti, inclusi i fornitori e le terze parti.

Sicurezza Coerente e Centralizzata: Le stesse policy di sicurezza (User-ID, App-ID, Advanced Threat Prevention) applicate a tutti gli utenti, su tutte le app, ovunque si trovino.

Visibilità End-to-End: Controllo completo sul traffico, sia verso Internet che verso le applicazioni private nel Data Center e nel cloud. Report e Logs presenti sull'unica console di gestione Strata Cloud Manager.

Semplificazione

Piattaforma Unificata: Drastica riduzione della complessità grazie al consolidamento di networking e sicurezza in un'unica soluzione gestita da una singola console: Strata Cloud Manager.

MTTD/MTTR Migliorati: Tempi medi di rilevamento e risoluzione dei problemi ridotti drasticamente grazie alla visibilità fornita da ADEM.

Abilitazione Rapida del Business: Apertura di nuove filiali o estensione a nuovi cloud (tramite ZTNA Connector) in tempi rapidissimi.

E se non si usasse SD-WAN?

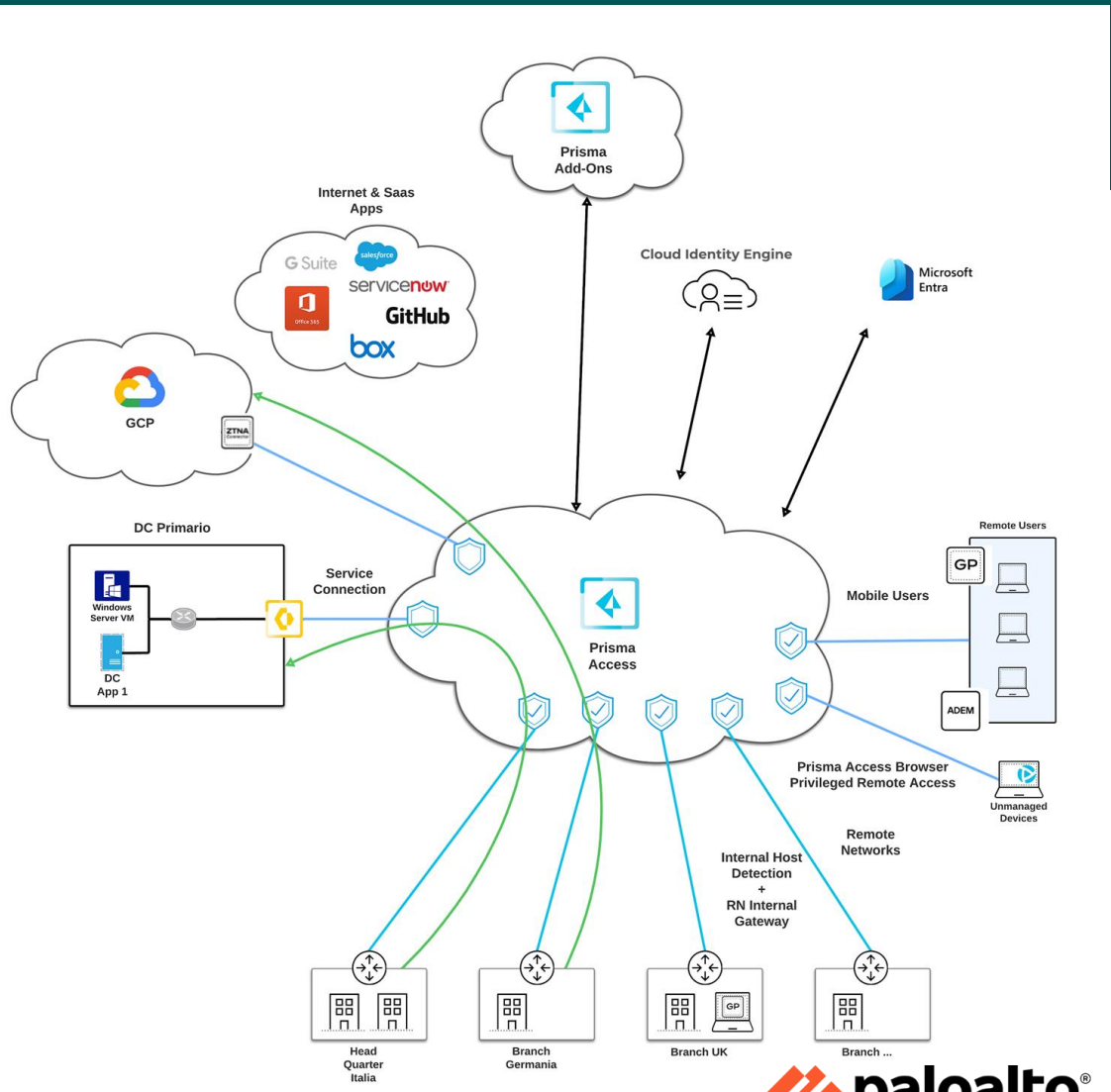
Punto di Partenza: Il cliente ha appena rinnovato i firewall delle sedi e non è disposto a un refresh tecnologico per installare apparati SD-WAN (ION).

L'esigenza principale è la sicurezza cloud-delivered, non l'ottimizzazione della WAN.

La Soluzione: Prisma Access come Backbone di Rete.

Le filiali si connettono a Prisma Access tramite tunnel IPsec standard, utilizzando i firewall (anche di terze parti) o i router già presenti in sede.

Risultato: Tutto il traffico delle filiali viene inoltrato a Prisma Access, che agisce come "hub di sicurezza" nel cloud, eliminando il backhauling verso il Data Center.



Cosa chiedere per qualificare l’opportunità

Capire il Business e le Sfide

1. Quali sono le principali sfide attuali (performance, sicurezza, costi) e quali obiettivi di business volete raggiungere con questa trasformazione?
2. Descrivete la distribuzione geografica dei vostri utenti (in ufficio, ibridi, full-remote) e delle vostre applicazioni (on-prem, IaaS, SaaS).

Analizzare lo Stato Attuale

3. Quale soluzione utilizzate oggi per l'accesso remoto (VPN)? Quali sono i suoi limiti?
4. Come gestite la connettività delle filiali (MPLS, Internet)?
5. Quale sistema usate per la gestione delle identità (es. Entra ID, Okta, AD on-prem)?
6. Come garantite l'accesso sicuro a utenti non-dipendenti (consulenti, fornitori, terze parti)?

Definire la Soluzione Futura

7. Quale esperienza di connessione volete per gli utenti (es. Always-On trasparente, On-Demand)?
8. Qual è lo scope del progetto? (Numero di utenti, numero di sedi, throughput).
9. Oltre agli utenti, è necessario connettere anche server/dispositivi headless?
10. Quali sono le tempistiche (deadline) e le priorità del progetto?

TD SYNNEX

“Security is a process, not a product”

Bruce Schneier

Q&A

PROSSIMI APPUNTAMENTI

7 NOVEMBRE: Obiettivo Passwordless con RSA

14 NOVEMBRE: Acronis Disaster Recovery

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: riccardo.tesi@tdsynnex.com
andrea.pezzoni@tdsynnex.com