ZTNA e ITDR secondo Sophos: come Zero Trust e la protezione dell’identità possono rafforzare la sicurezza

Walter Narisoni
Sophos
Settembre 2025

Il panorama delle minacce moderne non lascia spazio a errori

Velocità

Tempo mediano impiegato da un utente malintenzionato per ottenere l'accesso come amministratore di dominio

11 ore

Aumento

Aumento annuale degli strumenti " living-off-the-land " utilizzati negli attacchi

126%

Sofisticazione

Percentuale di attacchi in cui gli avversari hanno effettuato l'accesso con credenziali valide

56%

Ricerca sulle minacce Sophos X-Ops

SOPHOS

utenti

dati

ZERØ TRUST

dispositivi

UN MODELLO E UNA FILOSOFIA PER LA CYBERSECURITY

applicazioni / workloads

rete

SOPHOS

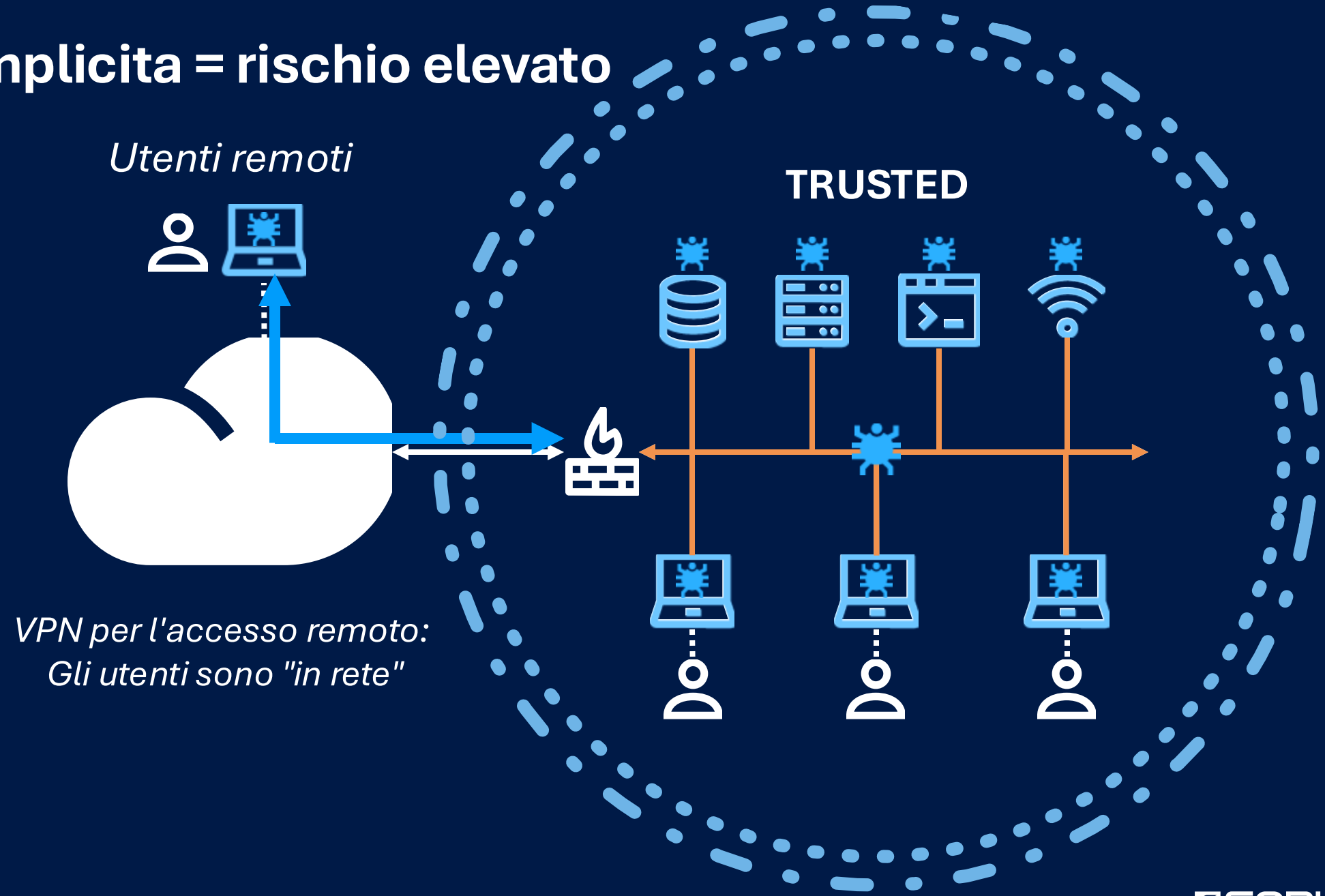
Zero Trust

Non fidarsi di nulla - Verifica tutto

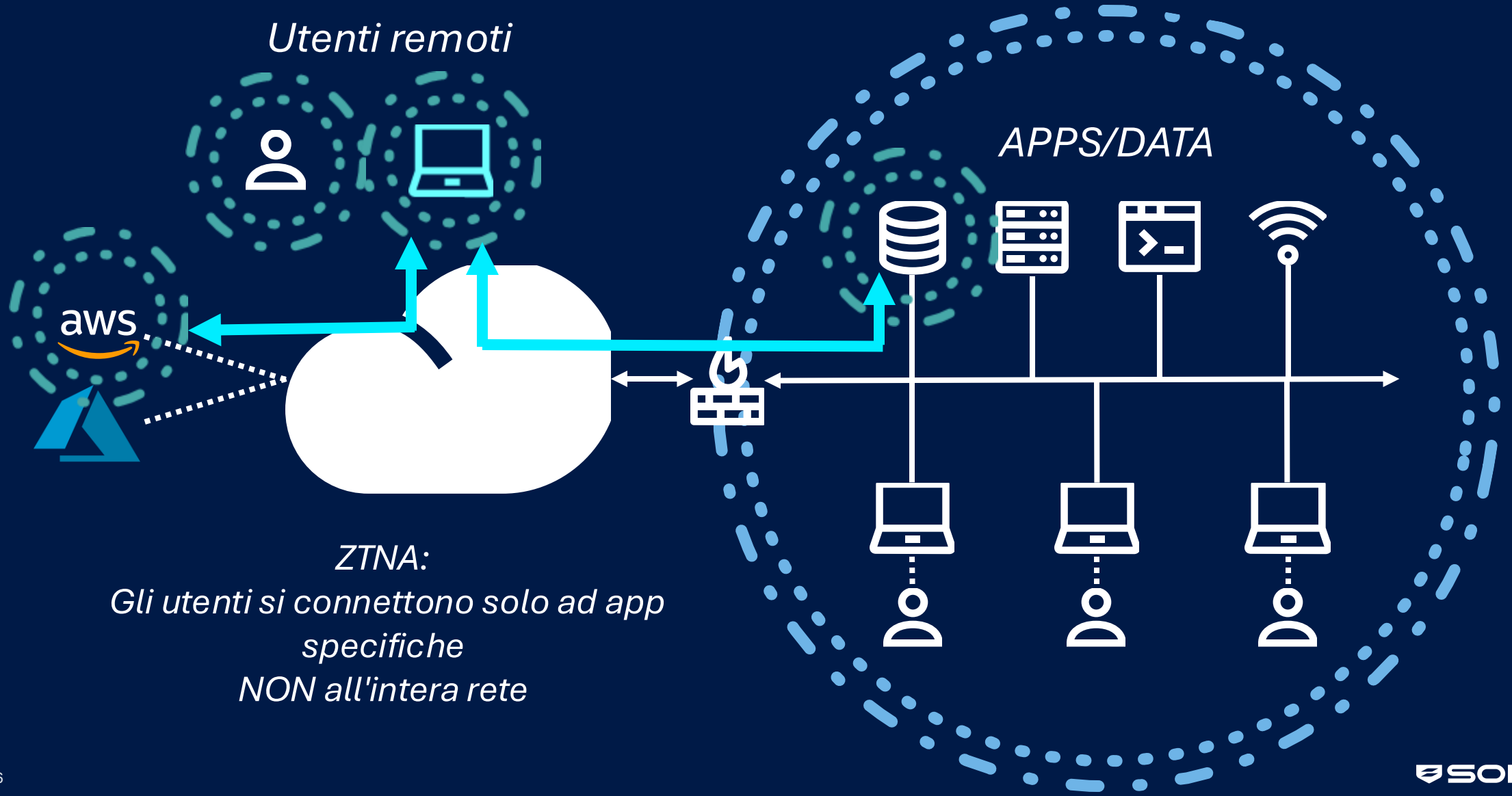
La fiducia si guadagna – non si dà

SOPHOS

Fiducia implicita = rischio elevato



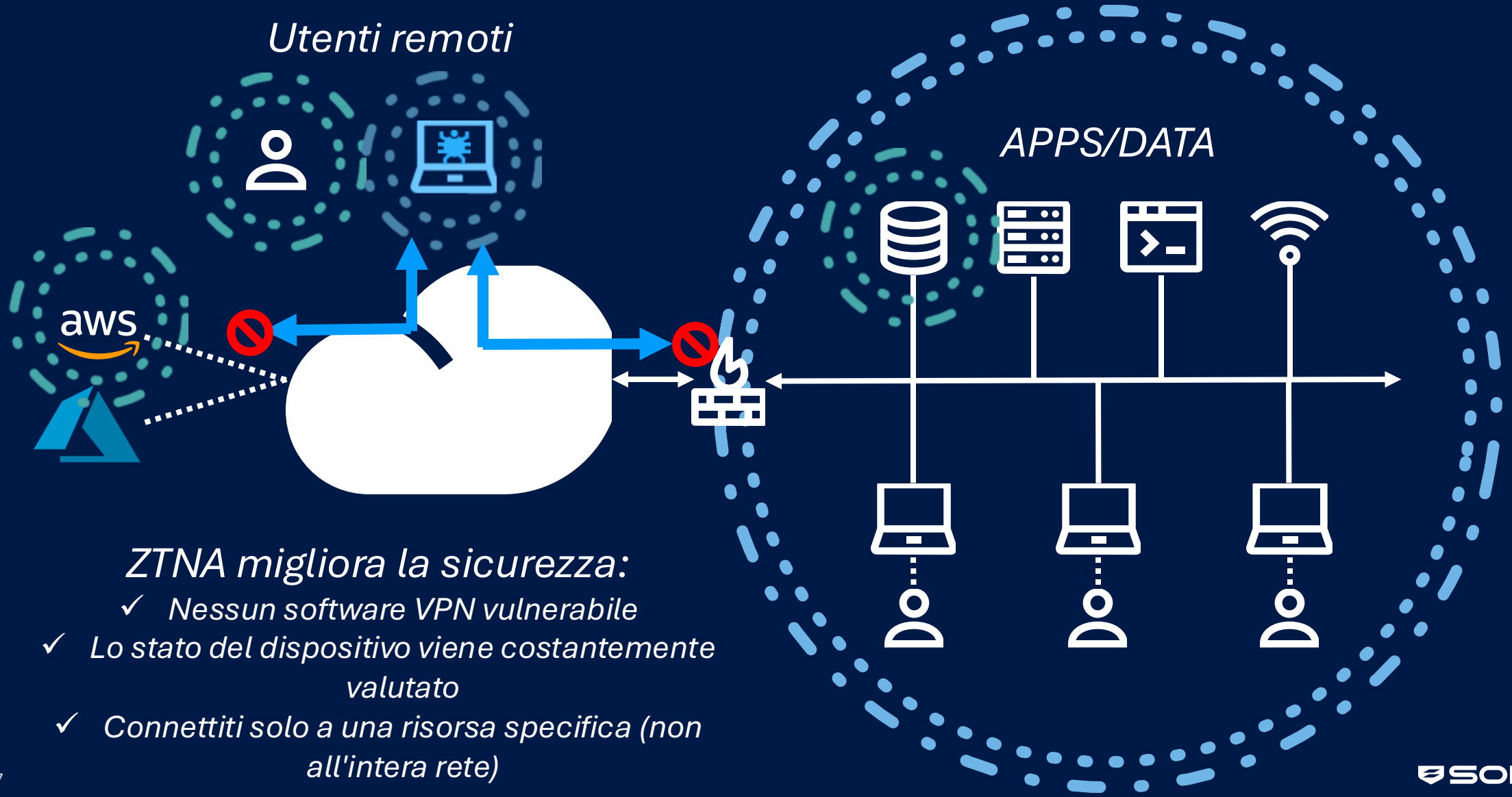
Accesso alle applicazioni di rete Zero Trust



ZTNA:
Gli utenti si connettono solo ad app specifiche
NON all'intera rete

SOPHOS

ZTNA ha migliorato la sicurezza – in modo drammatico!



ZTNA migliora la sicurezza:

- ✓ *Nessun software VPN vulnerabile*
- ✓ *Lo stato del dispositivo viene costantemente valutato*
- ✓ *Connettiti solo a una risorsa specifica (non all'intera rete)*

SOPHOS

I sei principali vantaggi dello ZTNA

1. Zero Trust - Nessuna fiducia implicita
- Ogni utente/dispositivo/app è il proprio perimetro
- Microsegmentazione delle applicazioni

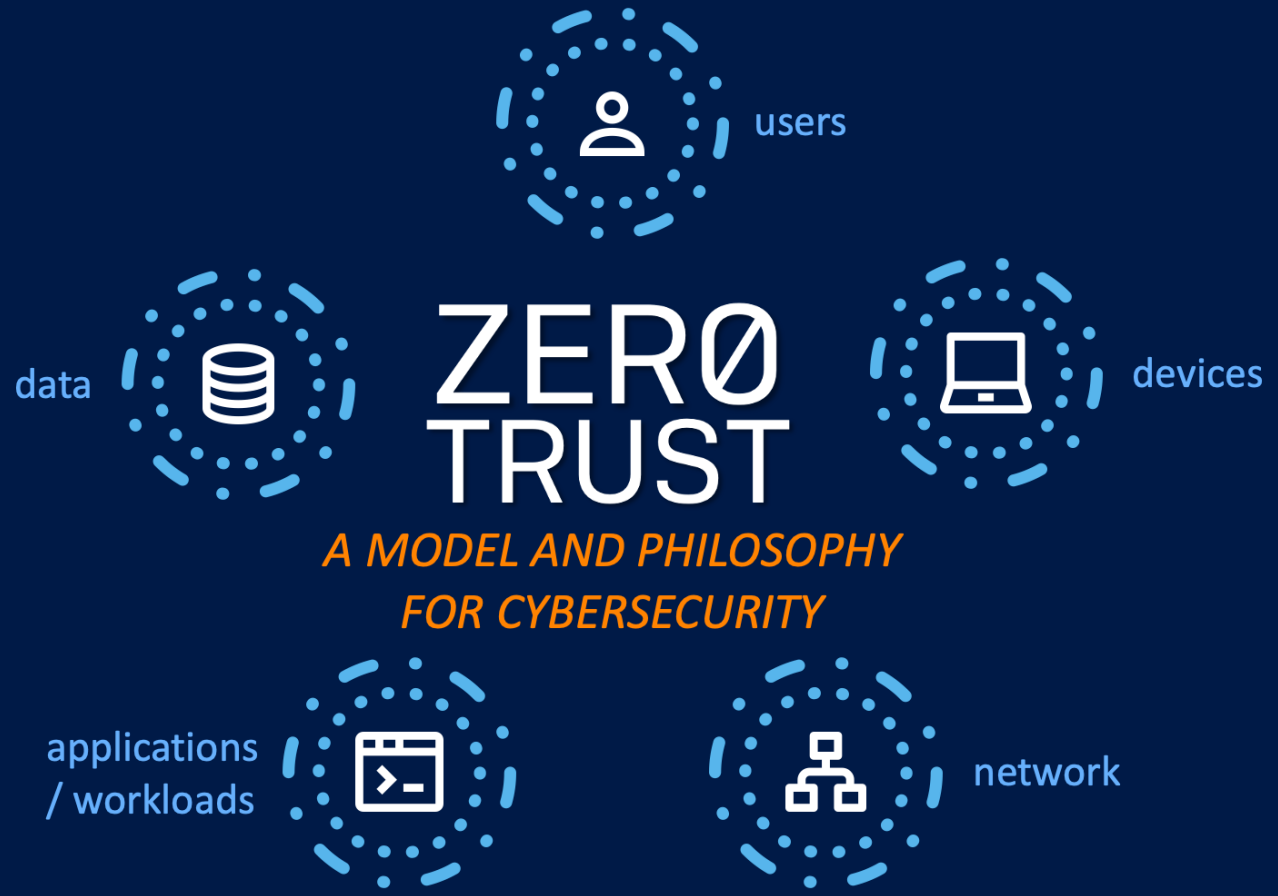
2. Integrità del dispositivo
- Controlla l'accesso in base alla conformità e all'integrità del dispositivo

3. Funziona ovunque
- Nella rete o fuori

4. Connettività trasparente
- Esperienza senza attriti, "funziona e basta"
- Semplificare le attività per gli utenti finali

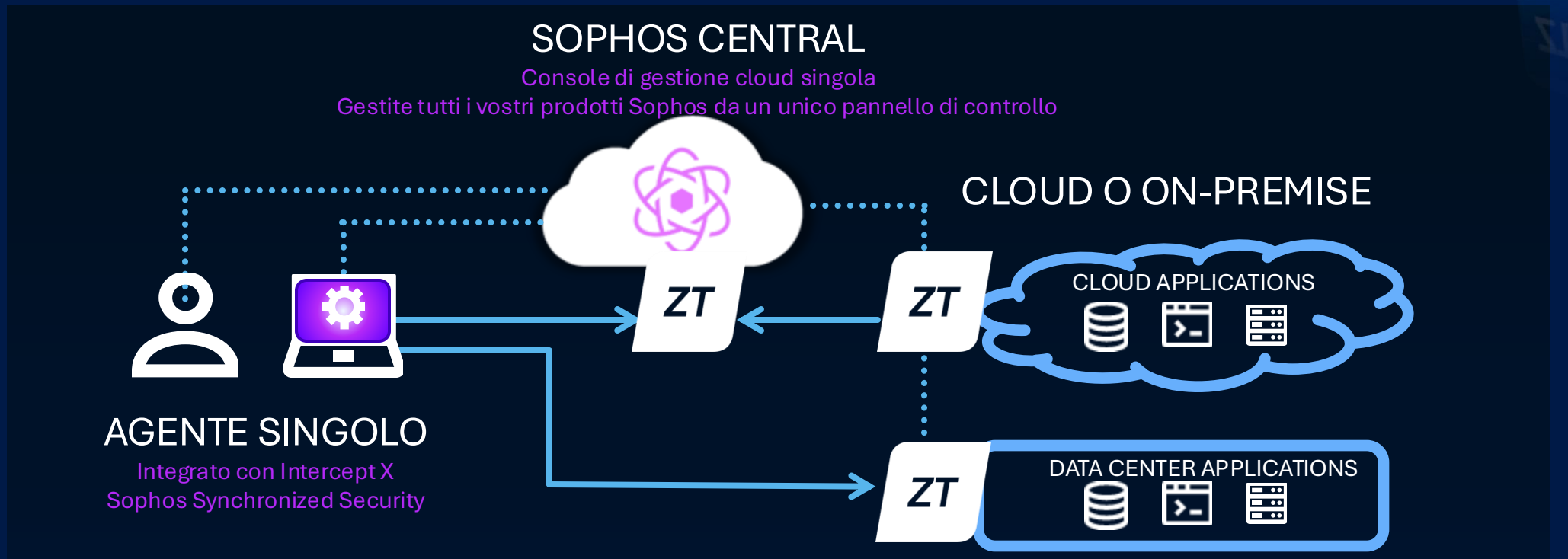
5. Migliore visibilità
- Informazioni dettagliate su accesso, stato, capacità e licenze delle app

6. Amministrazione più semplice
- Soluzione più snella e pulita
- Attiva rapidamente nuove app e registra gli utenti



Come funziona ZTNA?
A cosa serve?

ZTNA – Componenti chiave



ZTNA AGENT (o AGENTLESS)

- Integra continuamente l'identità e l'integrità dei dispositivi
- Accesso tramite browser senza agente per le app Web
- Supporto di Windows e macOS per thick client

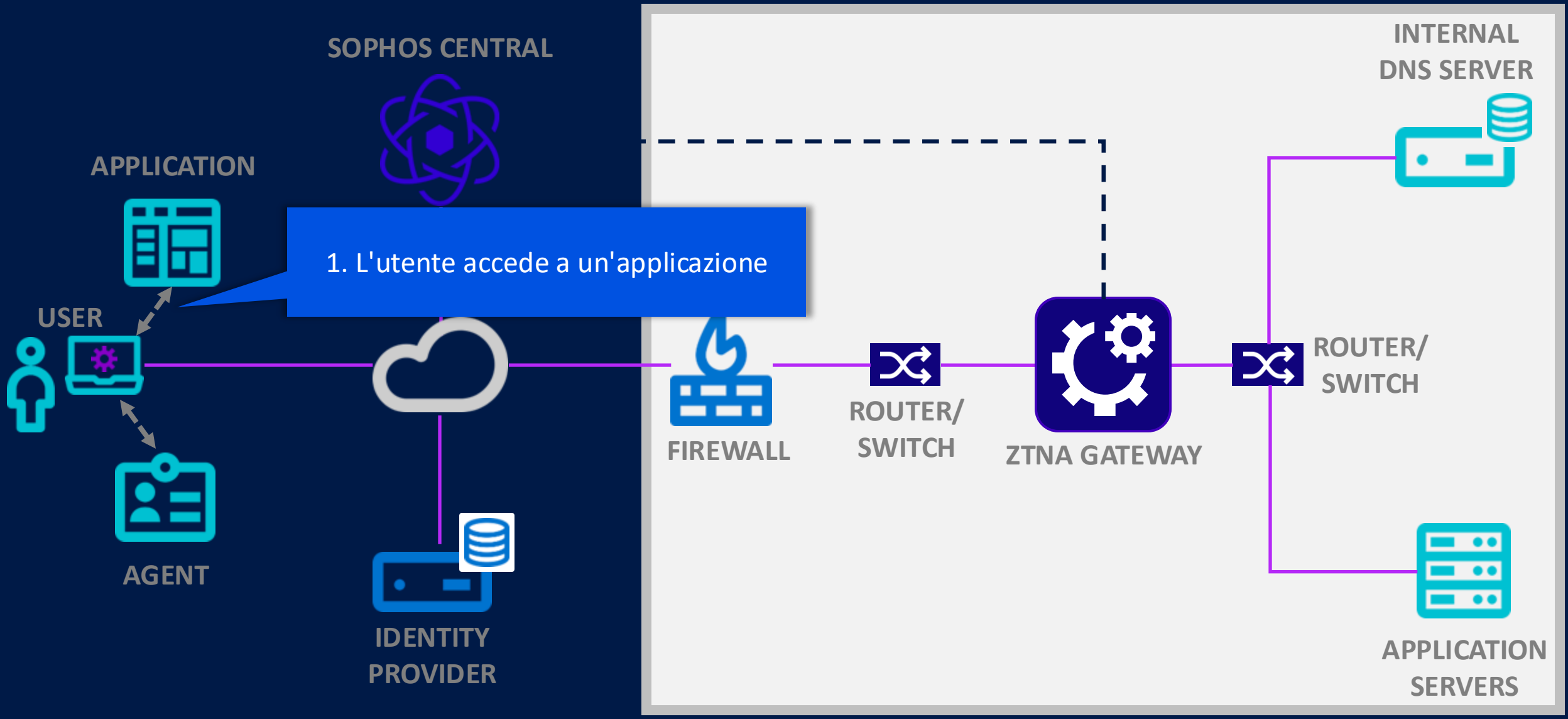
SOPHOS CENTRAL

- Gestione da un unico pannello di controllo
- Implementa facilmente ZTNA e Intercept X
- Controlli granulari delle policy
- Reportistica approfondita

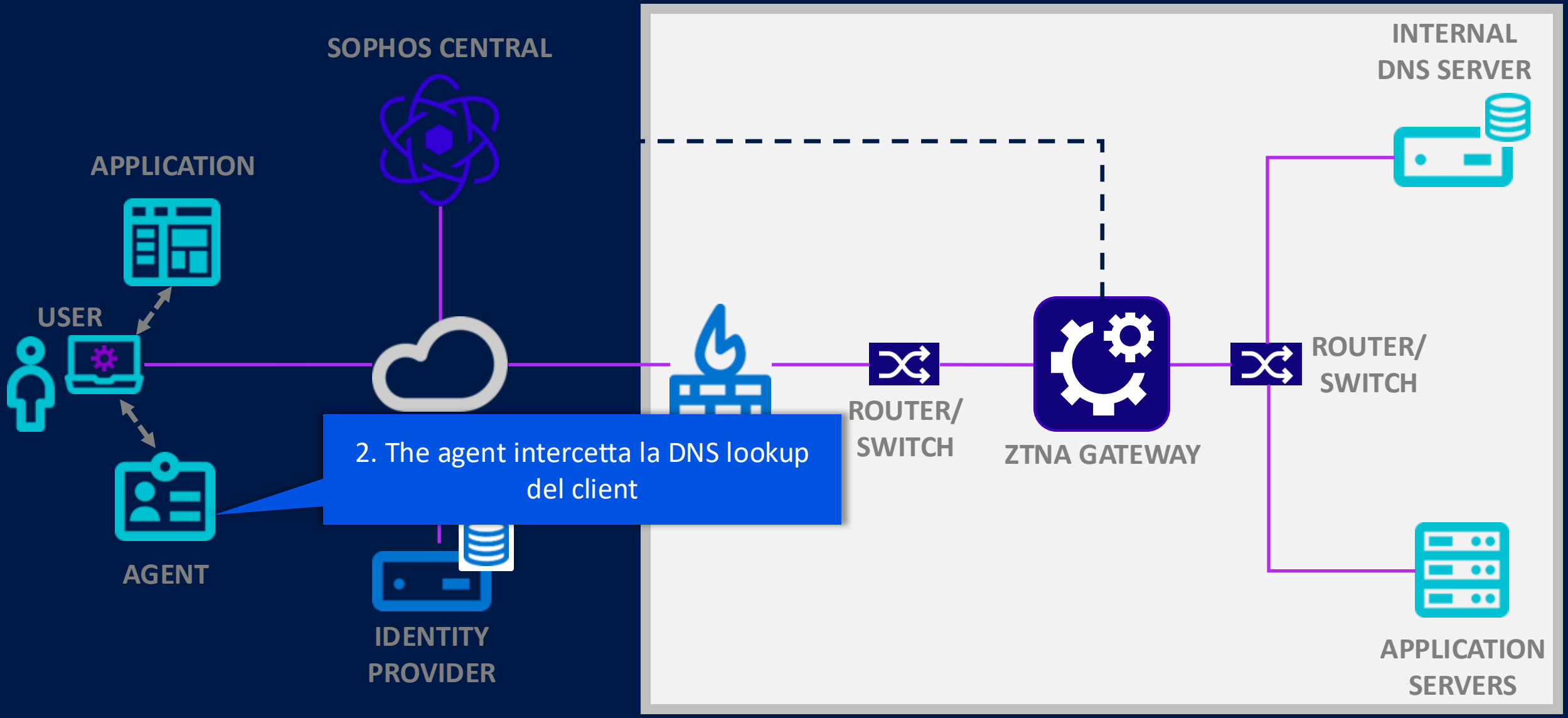
ZTNA GATEWAY

- Verifica e convalida l'accesso in modo intelligente e continuo in base alle policy
- On-premise o basato su cloud
- I gateway basati su cloud semplificano l'implementazione senza la necessità di configurare NAT del firewall
- Può combinare e abbinare gateway cloud o on-premise

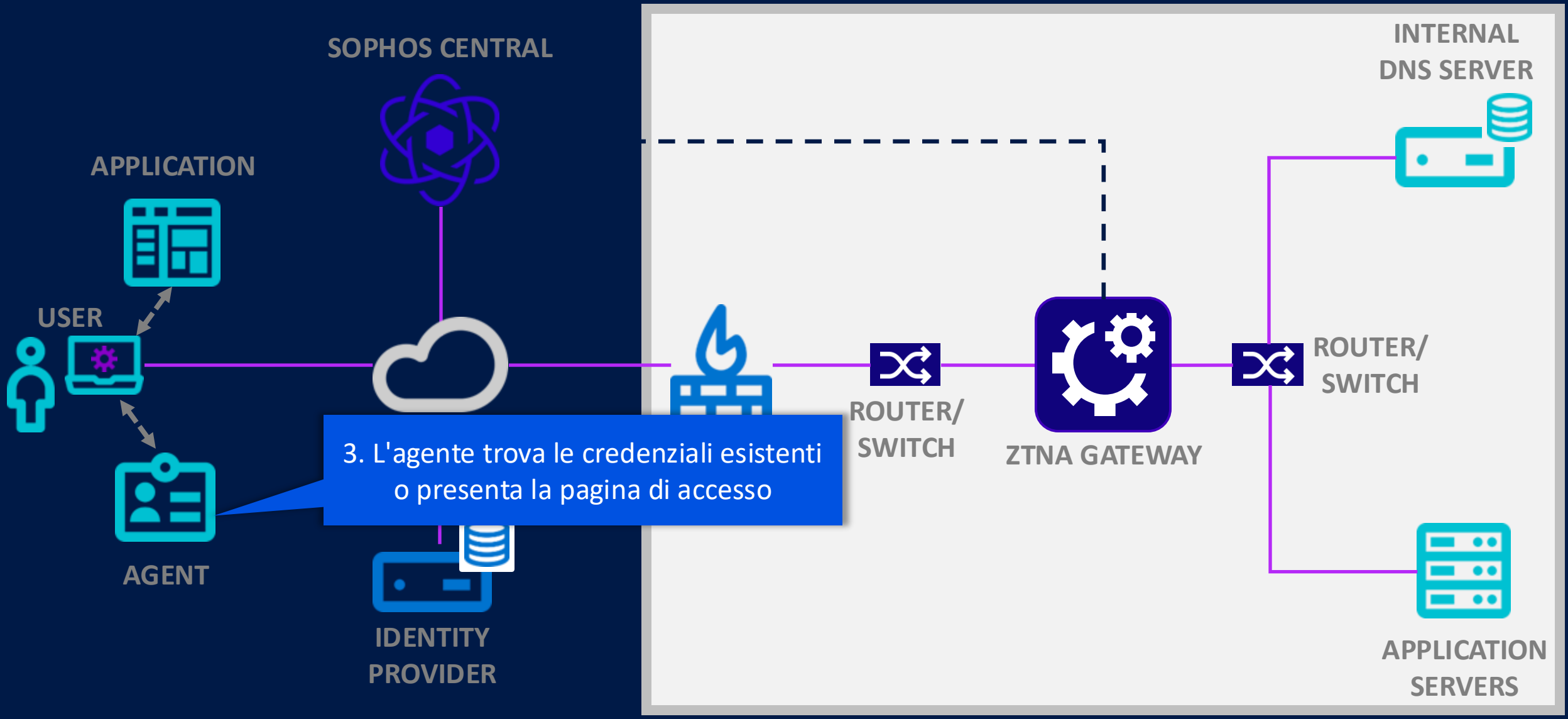
Agent Access



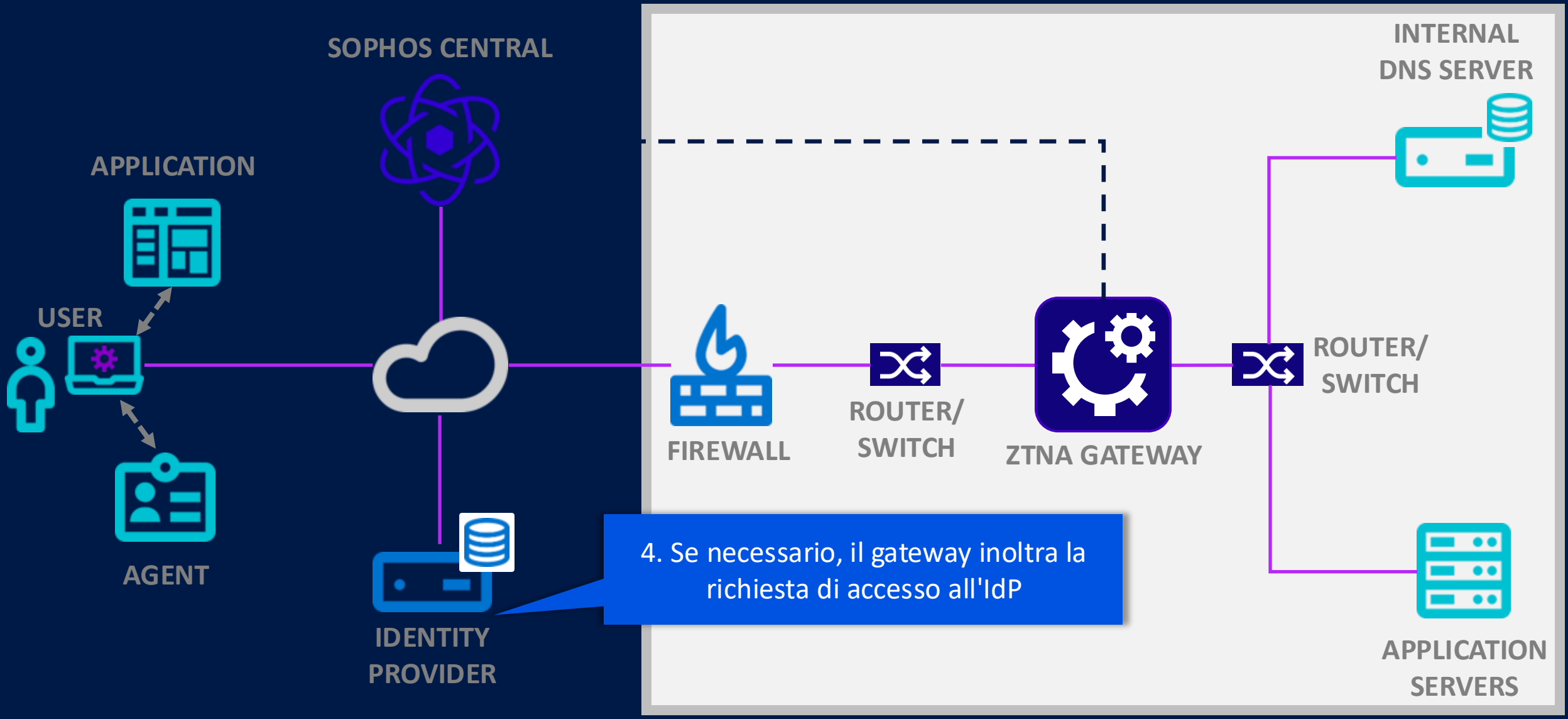
Agent Access



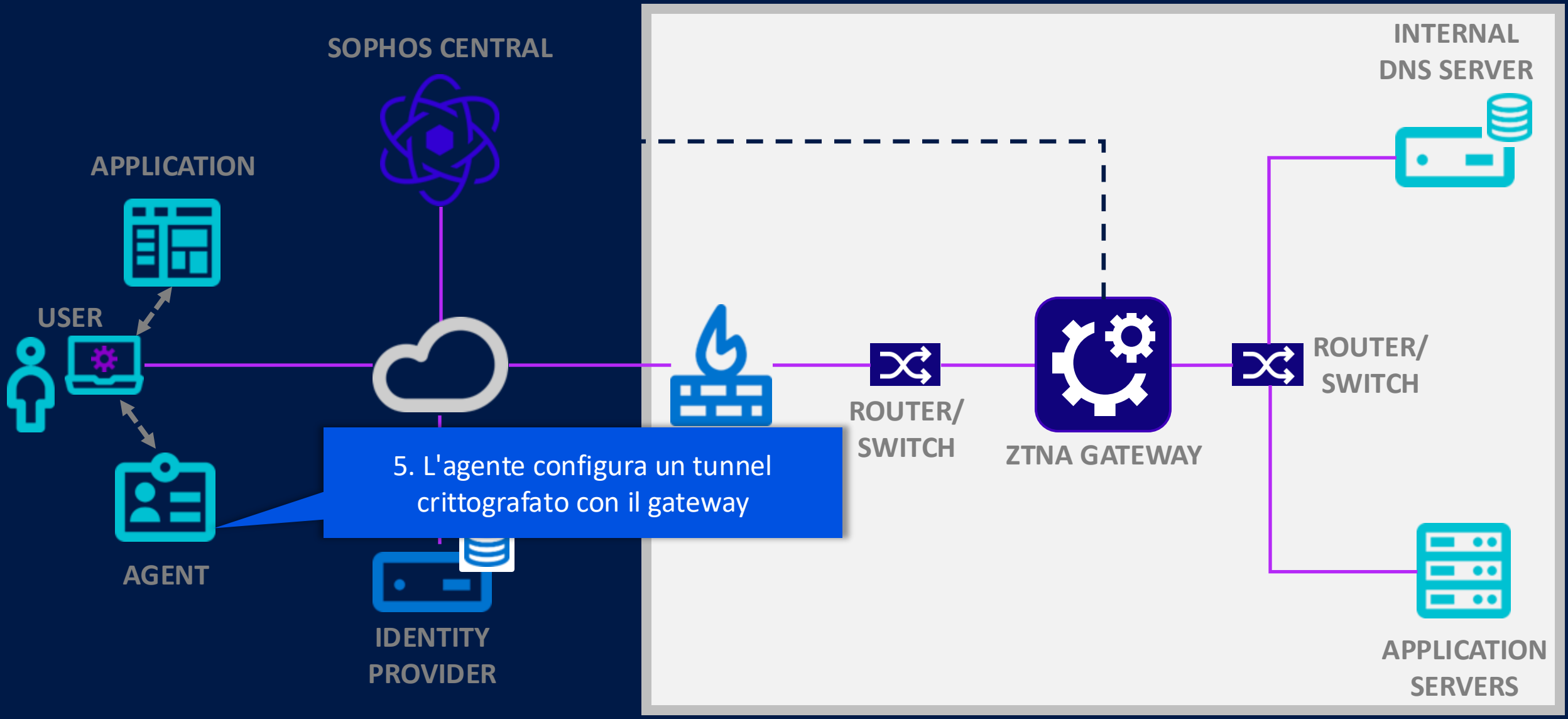
Agent Access



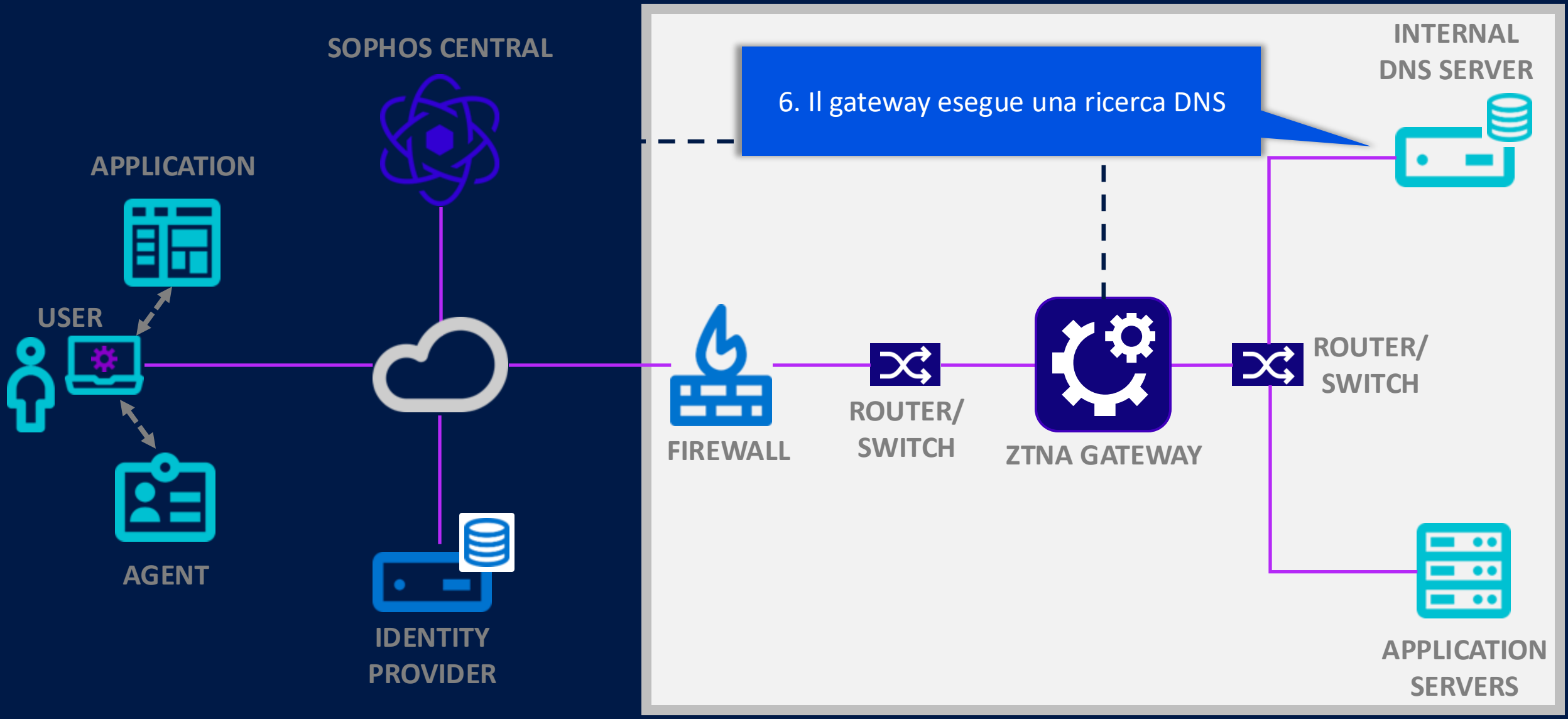
Agent Access



Agent Access

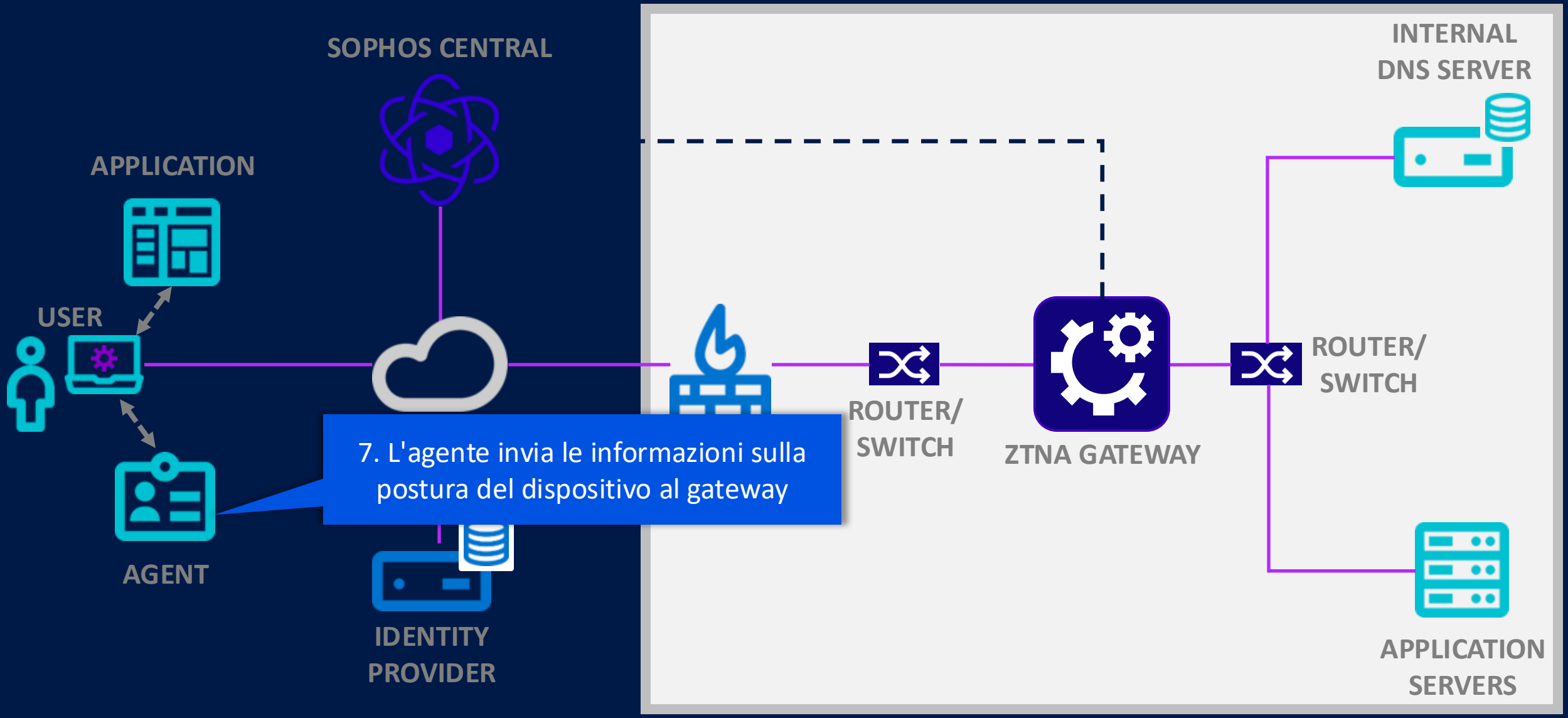


Agent Access

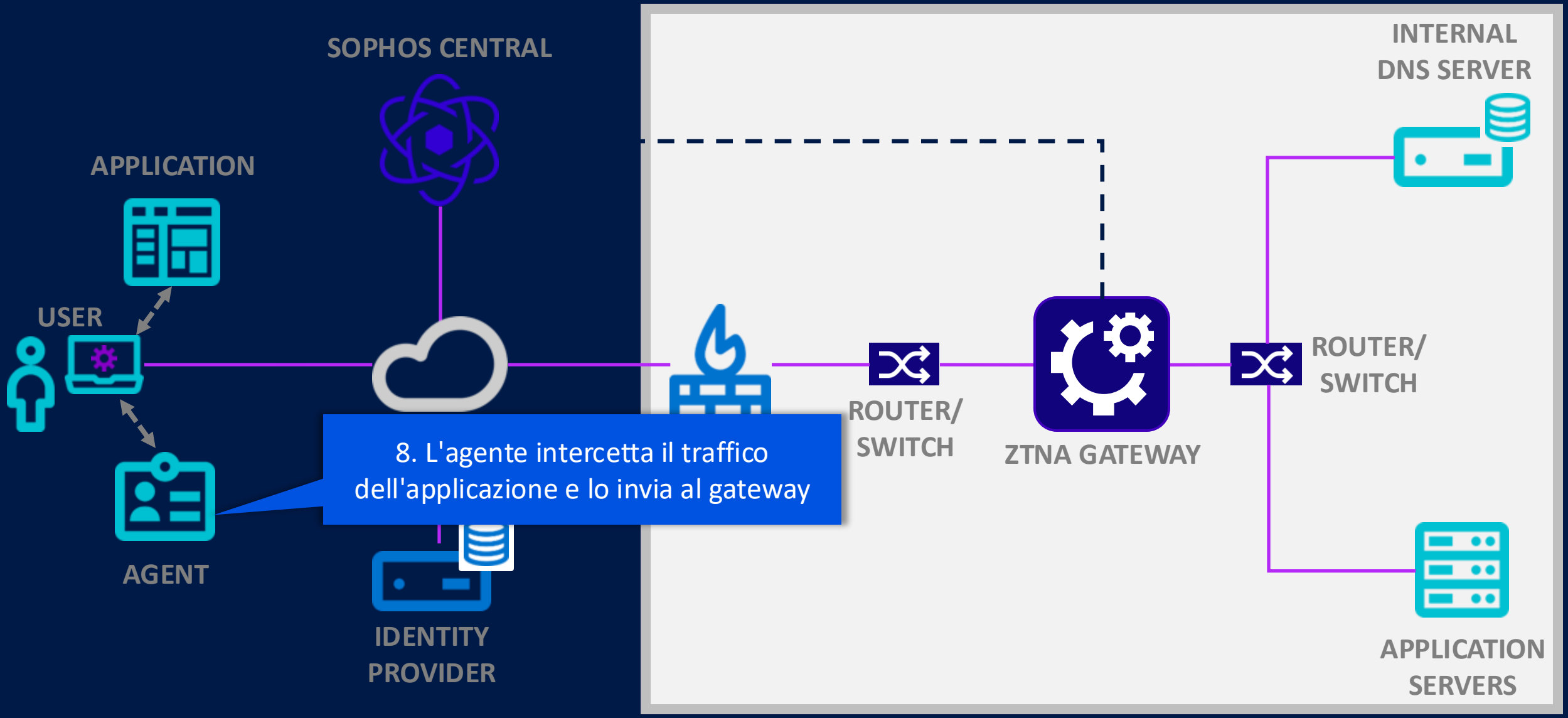


SOPHOS

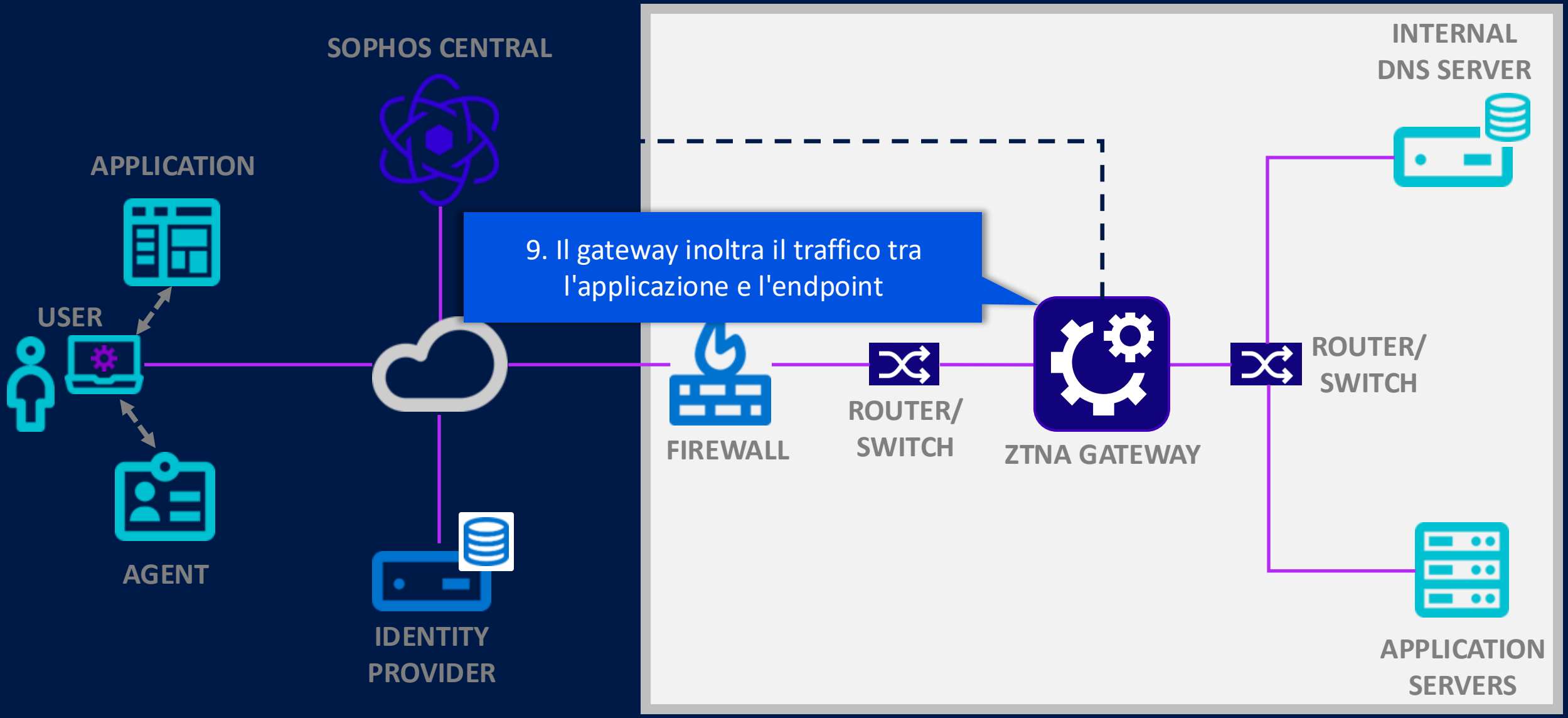
Agent Access



Agent Access



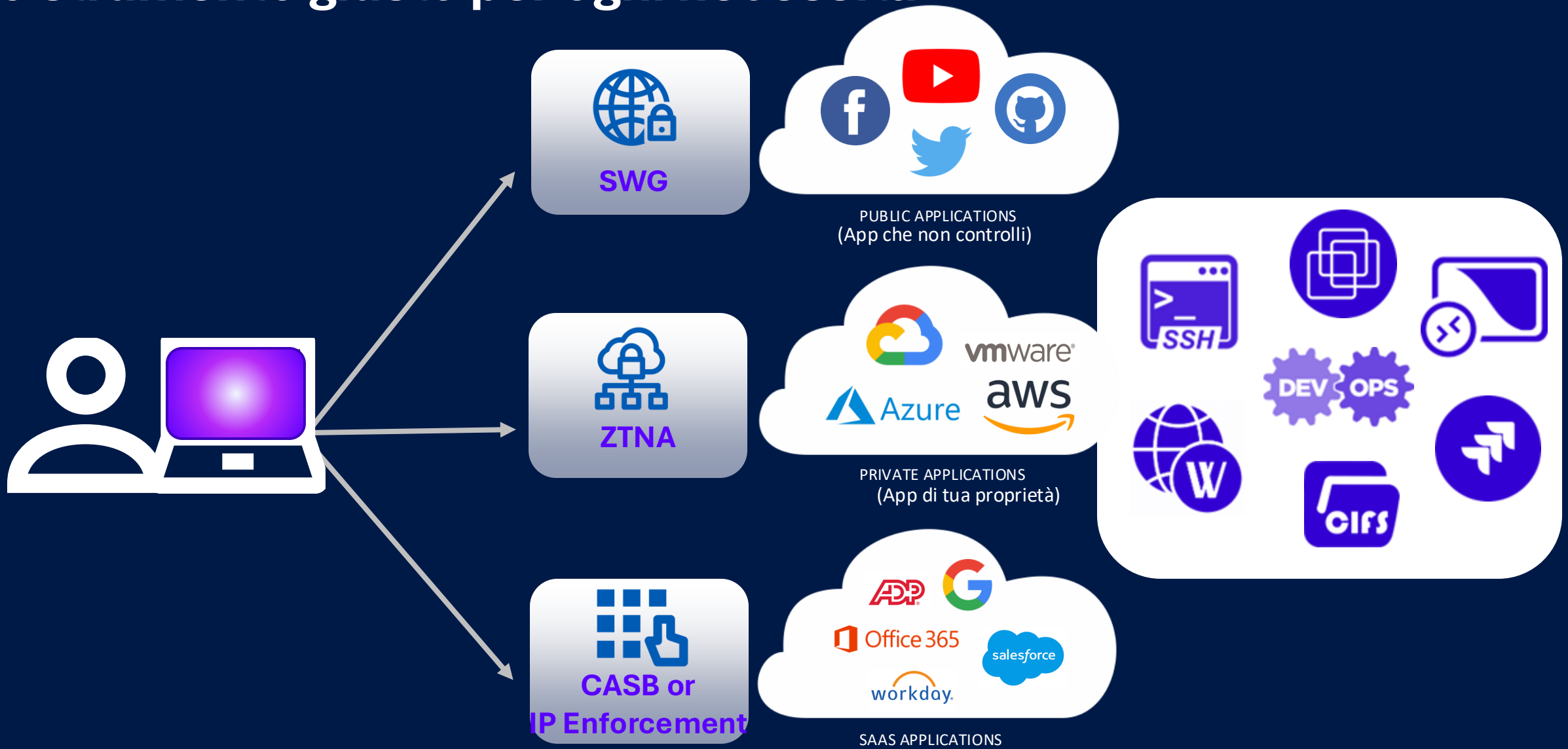
Agent Access



SOPHOS

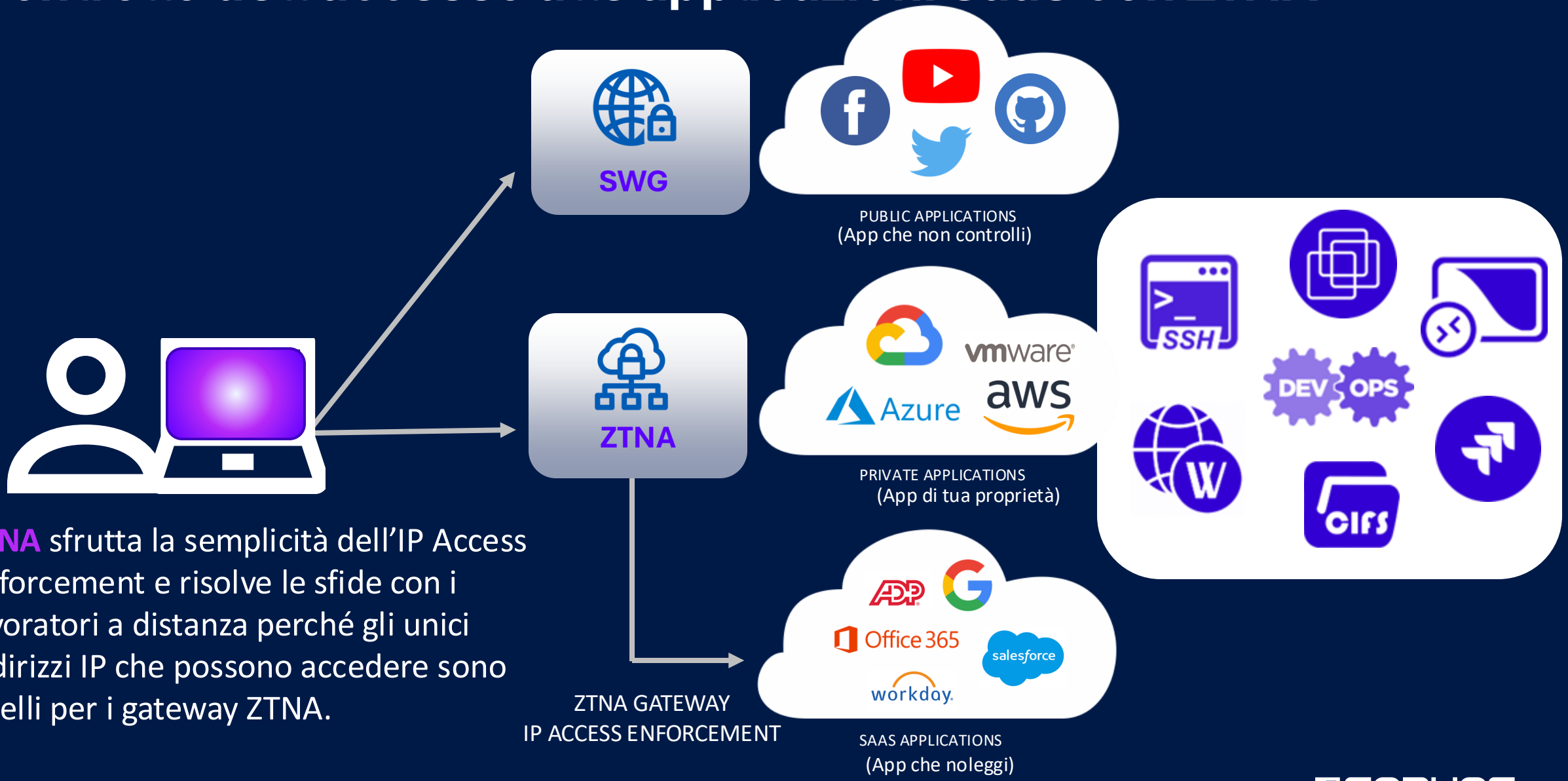
Quali tipi di app protegge ZTNA?

Lo strumento giusto per ogni necessità



SOPHOS

Controllo dell'accesso alle applicazioni SaaS con ZTNA



ZTNA sfrutta la semplicità dell'IP Access Enforcement e risolve le sfide con i lavoratori a distanza perché gli unici indirizzi IP che possono accedere sono quelli per i gateway ZTNA.

SOPHOS

Sophos Firewall

Secure By Design | Customer Security is our Top Priority

1 | BEST PRACTICE INTEGRATE

Garantire che il livello di sicurezza del firewall sia ottimale

- Distribuzione sicura e pronta all'uso con controlli di accesso rigorosi e granulari, regole firewall predefinite e protezione potente
- Funzionalità di sicurezza integrate come ZTNA proteggono le applicazioni, rendendole invisibili agli aggressori, consentendo al contempo l'accesso remoto sicuro

2 | HARDENING CONTRO L'ATTACCO

Prevenzione degli attacchi mirati al firewall

- Sophos Central cloud management offre una gestione remota sicura da qualsiasi luogo, senza esporre il firewall
- Supporto per l'autenticazione a più fattori (MFA), containerizzazione del portale VPN e di altri limiti di attendibilità, controlli predefiniti rigorosi, blocco dei paesi e altro ancora

3 | SUPPORTO AUTOMATICO DEGLI HOTFIX

Riduzione al minimo delle interruzioni causate dall'applicazione di patch

- La funzionalità di hotfix automatizzata integrata ci consente di inviare patch urgenti e importanti "over-the-air" per risolvere qualsiasi nuova vulnerabilità zero-day o altro problema sensibile
- Non richiede tempi di inattività normalmente associati agli aggiornamenti regolari del firmware

4 | MONITORAGGIO PROATTIVO

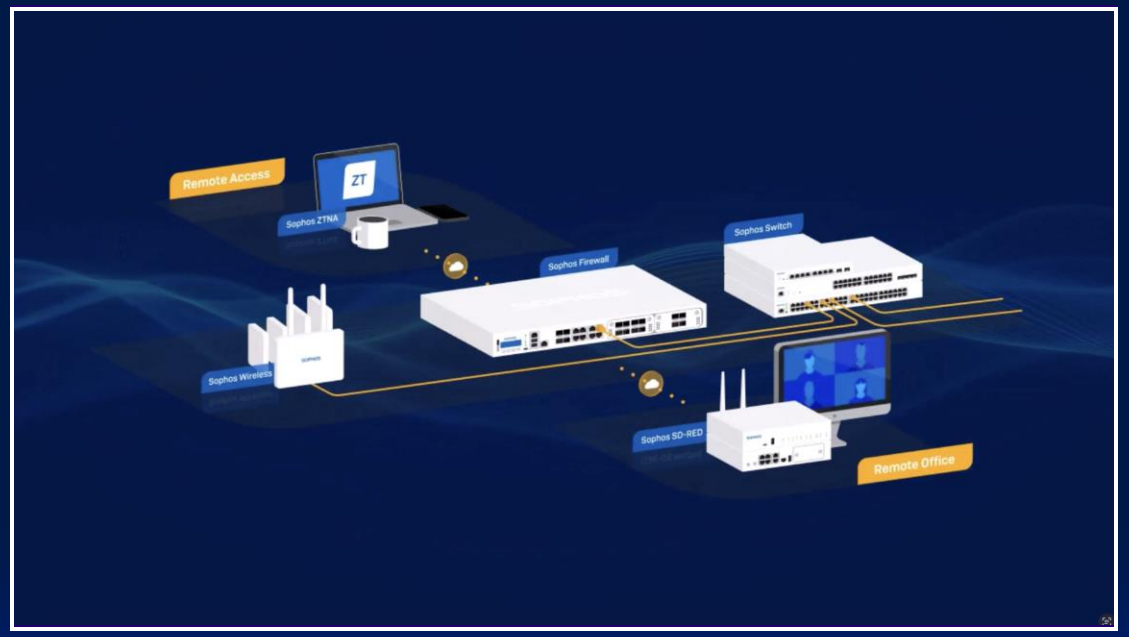
Essere proattivi, trasparenti e reattivi

- La continua ricerca di potenziali minacce nella nostra base di installazione globale di firewall dei clienti consente una risposta rapida a qualsiasi incidente
- Se il firewall di un cliente viene attaccato, lavoriamo velocemente per bloccare l'attacco e impedire che si verifichi altrove
- Uno dei migliori programmi di bug-bounty del settore

SOPHOS

Sophos Firewall v21.5

Più di un semplice firewall



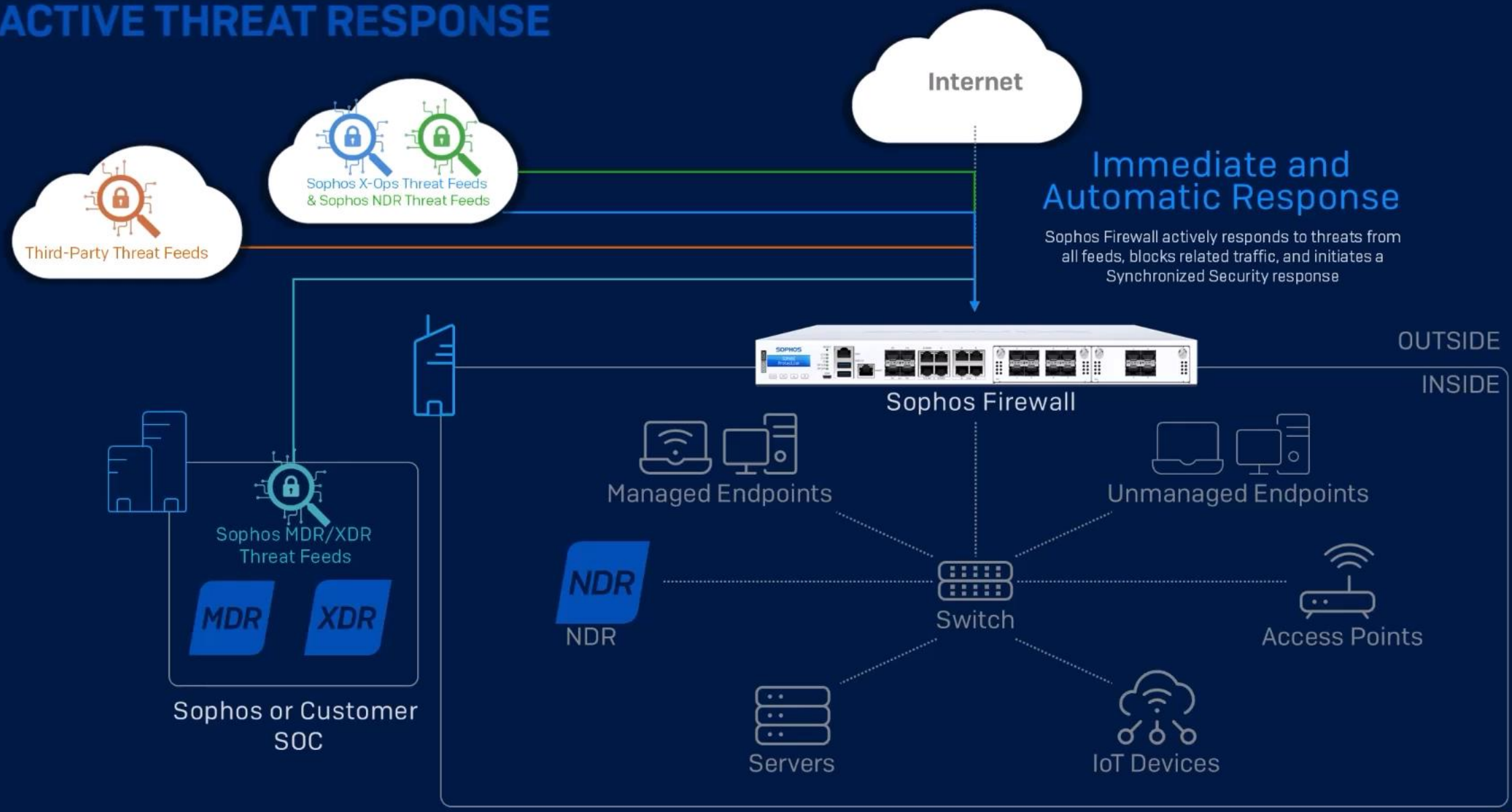
Protezione ZTNA e DNS integrata

Sicurezza sincronizzata evoluta con Active Threat Response

Network Detect and Response essentials integrata

SOPHOS

ACTIVE THREAT RESPONSE



Sophos ITDR

Monitora continuamente gli ambienti per rilevare rischi di identità ed errori di configurazione

Punti deboli dei clienti

Identity
è il carburante dell'ecosistema criminale informatico

$4.8M

Costo medio di una violazione dei dati, di cui il 79% è correlato all'identità.

91%

Le organizzazioni che hanno subito una violazione dell'identità negli ultimi 12 mesi

95%

Le organizzazioni che hanno una configurazione errata dell'identità che consente l'escalation dei privilegi.

1. Based on Secureworks' data gathered from thousands of incident response engagements conducted by the Secureworks CTU℠
2. Based on internally collected data by the Secureworks CTU
3. Identity Defined Security Alliance (IDSA), 2024 Trends in Securing Digital Identities

SOPHOS

Il nostro approccio olistico alla riduzione del rischio di identità

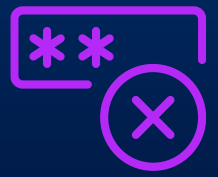
Protegge dalle minacce all'identità

Rileva e risponde automaticamente alle sofisticate minacce basate sull'identità

Riduce la superficie di attacco dell'identità

Scansiona continuamente Microsoft Entra ID per identificare lacune di sicurezza

Riduce al minimo il rischio di furto delle credenziali



Monitora e avvisa quando le credenziali sono state esposte

Identifica i comportamenti rischiosi degli utenti

Monitora l'attività anomala associata al furto delle credenziali

XDR

ITDR

SOPHOS

Caratteristiche principali di Sophos ITDR

Scopri i rischi per l'identità <90 secondi

- Identifica le lacune di sicurezza in Microsoft Entra ID
- Identity Posture
- Dashboard con punteggio di rischio posturale
- Elenco dei risultati con priorità
- Catalogo di utenti, dispositivi, applicazioni e gruppi

Monitora le credenziali trapelate o rubate

- Identifica le credenziali trapelate o rubate
  - Dark web
  - Violazioni di terze parti

Identificare il comportamento rischioso degli utenti

- Rileva gli utenti che mostrano modelli di comportamento rischiosi per ulteriori indagini.

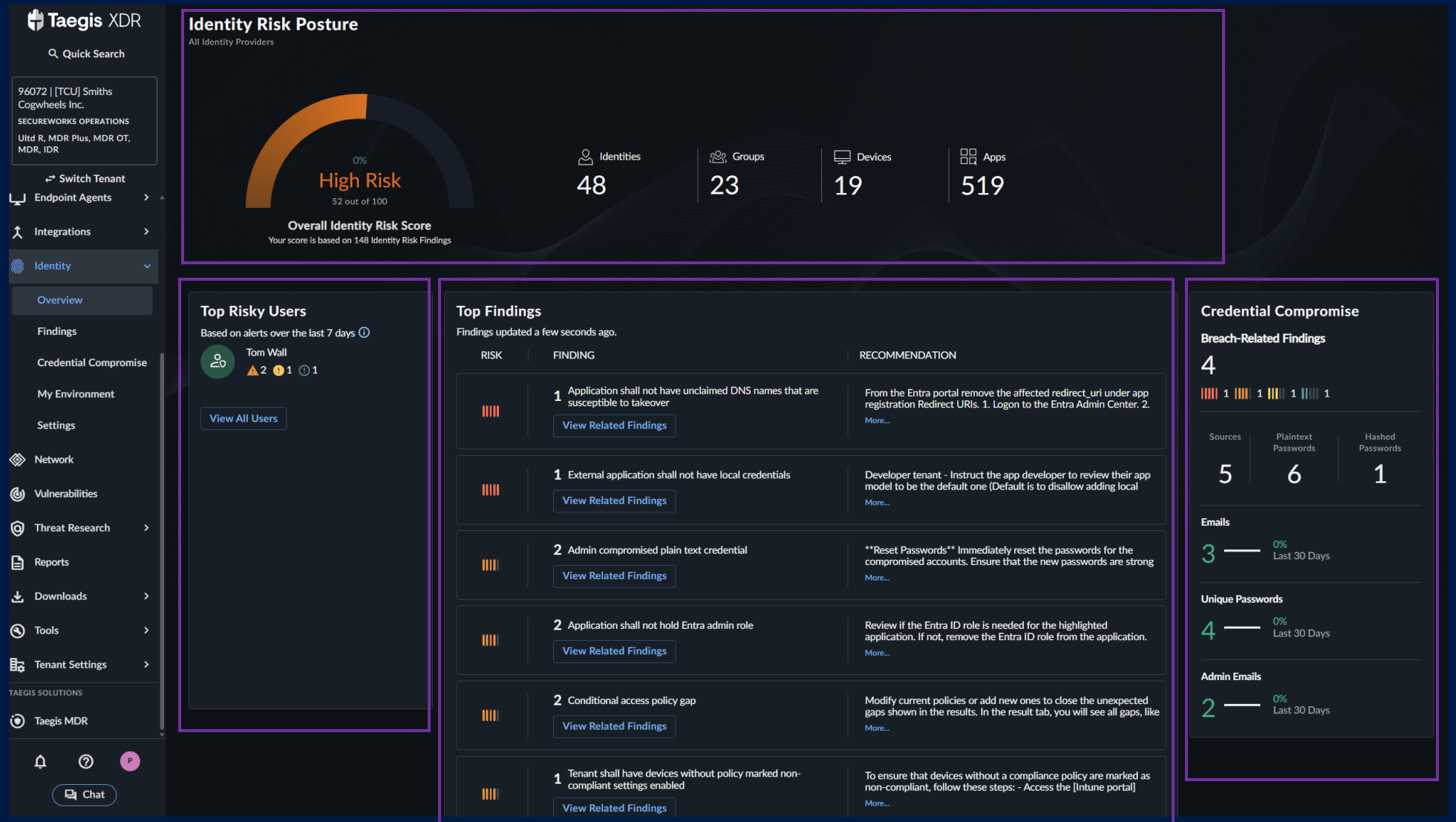
Detection & Response Playbooks

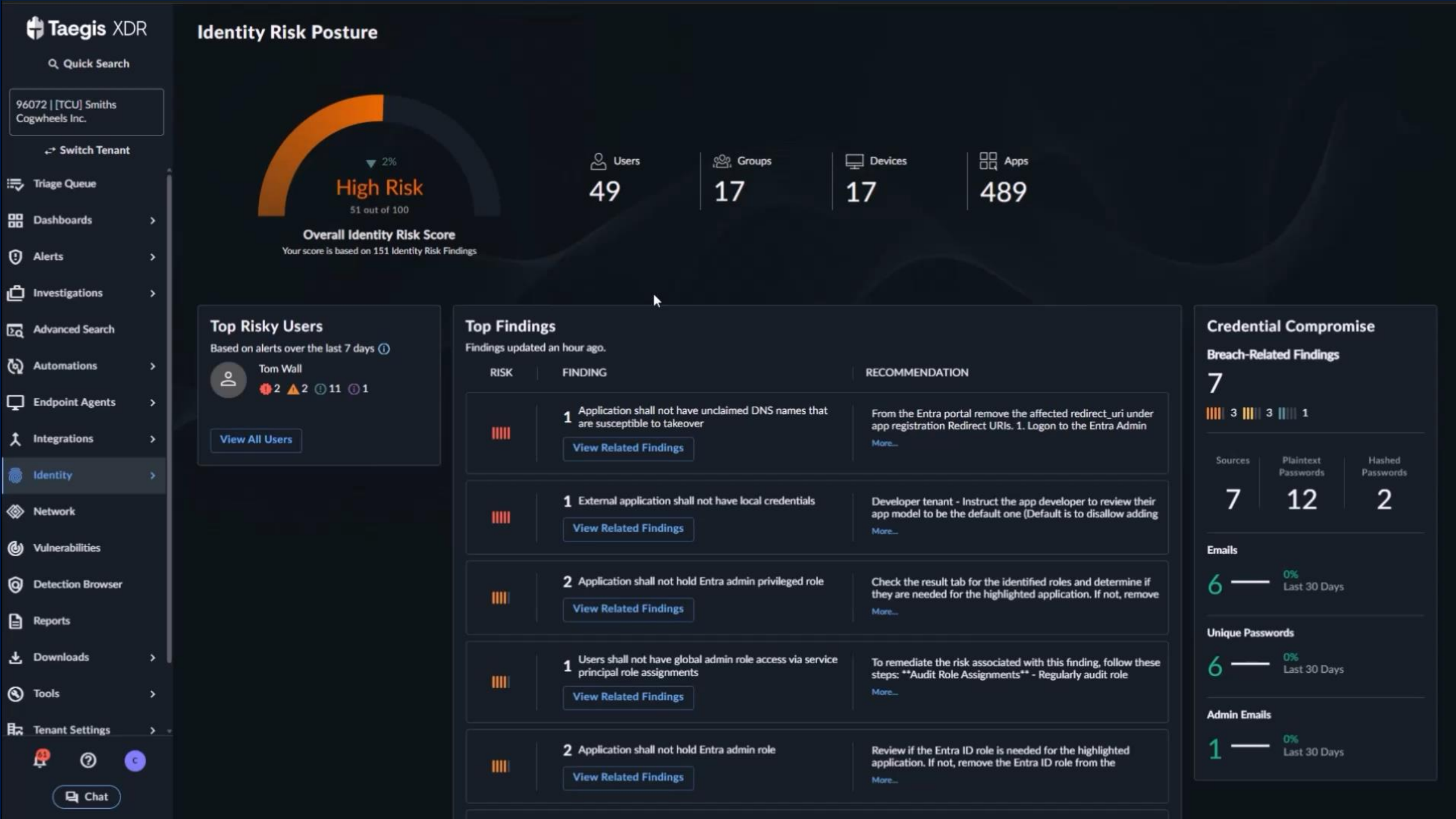
- Taegis Detectors
  - Credenziali rubate, kerberoasting, viaggi impossibili, ecc..
- Automated playbooks
  - Reimposta la password, blocca l'account, disabilita l'utente, forza il ripristino dell'MFA, ecc.

Riduzione del rischio

SOPHOS

Panoramica delle funzionalità ITDR - Dashboard




Taegis XDR
Quick Search
96072 | [TCU] Smiths Cogwheels Inc.
Switch Tenant
Triage Queue
Dashboards
Alerts
Investigations
Advanced Search
Automations
Endpoint Agents
Integrations
Identity
Network
Vulnerabilities
Detection Browser
Reports
Downloads
Tools
Tenant Settings
Chat
Identity Risk Posture
2%
High Risk
51 out of 100
Overall Identity Risk Score
Your score is based on 151 Identity Risk Findings
Users
49
Groups
17
Devices
17
Apps
489
Top Risky Users
Based on alerts over the last 7 days
Tom Wall
2 2 11 1
View All Users
Top Findings
Findings updated an hour ago.
RISK
FINDING
RECOMMENDATION
1 Application shall not have unclaimed DNS names that are susceptible to takeover
View Related Findings
From the Entra portal remove the affected redirect_uri under app registration Redirect URIs. 1. Logon to the Entra Admin
More...
1 External application shall not have local credentials
View Related Findings
Developer tenant - Instruct the app developer to review their app model to be the default one (Default is to disallow adding
More...
2 Application shall not hold Entra admin privileged role
View Related Findings
Check the result tab for the identified roles and determine if they are needed for the highlighted application. If not, remove
More...
1 Users shall not have global admin role access via service principal role assignments
View Related Findings
To remediate the risk associated with this finding, follow these steps: **Audit Role Assignments** - Regularly audit role
More...
2 Application shall not hold Entra admin role
View Related Findings
Review if the Entra ID role is needed for the highlighted application. If not, remove the Entra ID role from the
More...
Credential Compromise
Breach-Related Findings
7
3 3 1
Sources
7
Plaintext Passwords
12
Hashed Passwords
2
Emails
6
0%
Last 30 Days
Unique Passwords
6
0%
Last 30 Days
Admin Emails
1
0%
Last 30 Days

ITDR per Taegis XDR/MDR

Disponibile ora

Sophos ITDR per Sophos XDR/MDR

Ottobre 2025

Advisory Services Team

Sophos Advisory Services Team

TEAMS

60+

Tester dedicati

SUPPORTED BY:

400+

Security Analysts

250+

Threat Intel and research specialists

RICONOSCIMENTI

BACKGROUND

- Esperti di legge
- Militari
- Intelligence Community
- SANS Autori / Docenti
- Sviluppatori
- Esperti riconosciuti
- Civil Engineers
- Esperti OT
- Centinaia di certificazioni

SOPHOS

Advisory Services

Advisory Services Summary

Tipo di valutazione	Focus	Risponde alle domande chiave	Scenari di esempio
Penetration Testing Esterno	Sistemi accessibili da Internet: siti web, VPN e servizi rivolti al pubblico	Cosa può vedere e accedere un utente malintenzionato da Internet? Ci sono esposizioni non intenzionali?	Test di siti Web e servizi rivolti al pubblico; Identificazione delle vulnerabilità prive di patch
Penetration Testing Interno	Sistemi, applicazioni e dati all'interno della rete interna	Cosa potrebbe fare un utente malintenzionato se riuscisse ad accedere alla nostra rete? Potremmo rilevarli?	Testare la facilità con cui una minaccia interna può aumentare i privilegi ed esfiltrare i dati
Penetration Testing Rete Wireless	Infrastruttura Wi-Fi, protocolli di crittografia, autenticazione e controlli di accesso	La nostra rete wireless è sicura? Ci sono dispositivi non autorizzati o rogue?	Test della sicurezza Wi-Fi dell'ufficio; identificare i punti di accesso non autorizzati; Tentativo di connessioni non autorizzate
Valutazione della sicurezza delle applicazioni Web	Difetti di codifica, autenticazione e gestione delle sessioni, controllo degli accessi	Le nostre app sono sicure? I dati sensibili sono esposti? Come possiamo correggere le vulnerabilità?	Test di portali clienti, siti di e-commerce, web app interne; identificazione di SQL injection, XSS o difetti di autenticazione

Cosa è incluso nel report

Sintesi
Destinato agli stakeholder non tecnici: alta dirigenza, revisori dei conti, consiglio di amministrazione e altri dipartimenti importanti.

Risultati dettagliati
Scritto per il personale tecnico per fornire risultati e raccomandazioni approfondite.

Metodologia di engagement
Definisce l'ambito dell'incarico e quali attività di test sono state eseguite.

Narrativo
Descrive la sequenza di azioni intraprese dai tester per raggiungere gli obiettivi dell'impegno, per aiutare a comprendere le minacce miste e/o le fasi dipendenti.

Consigli
Dettagli risultati, collegamenti a pagine Web per ulteriori letture e raccomandazioni per la correzione o la riduzione del rischio. I tester forniscono prove dei loro risultati e, se possibile, informazioni sufficienti per replicare i risultati utilizzando strumenti disponibili al pubblico.

Gamma di servizi

Affrontare una gamma completa di Security Use Cases

"Vogliamo migliorare la nostra prontezza di risposta agli incidenti."

"Abbiamo bisogno di monitoraggio, indagine e risposta agli incidenti 24 ore su 24, 7 giorni su 7".

"Abbiamo bisogno di supporto per la risposta agli incidenti di emergenza e di un'indagine completa".

"Vogliamo un team in attesa che ci aiuti in caso di incidente".

Un menu completo di servizi che consentono alle organizzazioni di valutare e migliorare la propria sicurezza e la preparazione agli incidenti

- Valutazioni e test di policy e capacità di reazione.
- Revisioni e sviluppo del piano degli incidenti.
- Formazione, esercizi e workshop.

Affrontare una gamma completa di Security Use Cases

"Vogliamo migliorare la nostra prontezza di risposta agli incidenti".

"Abbiamo bisogno di monitoraggio, indagine e risposta agli incidenti 24 ore su 24, 7 giorni su 7".

"Abbiamo bisogno di supporto per la risposta agli incidenti di emergenza e di un'indagine completa".

"Vogliamo un team pronto ad aiutarci in caso di incidente."

Monitoraggio 24 ore su 24, 7 giorni su 7, ricerca delle minacce, indagine e risposta agli incidenti forniti da un team di esperti come servizio completamente gestito.

- Le ricerche alle minacce scoprono le minacce che gli strumenti possono non notare.
- Gli analisti rispondono alle minacce in pochi minuti.
- Identifica la causa principale delle minacce e degli incidenti.

SOPHOS

Affrontare una gamma completa di Security Use Cases

"Vogliamo migliorare la nostra prontezza di risposta agli incidenti".

"Abbiamo bisogno di monitoraggio, indagine e risposta agli incidenti 24 ore su 24, 7 giorni su 7".

"Abbiamo bisogno di supporto per la risposta agli incidenti di emergenza e di un'indagine completa."

"Vogliamo un team in attesa che ci aiuti in caso di incidente".

Risposta agli incidenti di emergenza per eliminare rapidamente le minacce attive, identificare la causa principale e monitorare il ripetersi.

- Implementazione rapida per valutare ed eliminare le minacce.
- Digital forensics per identificare l'ambito e la causa principale.
- Monitoraggio e risposta continui alle minacce.

SOPHOS

Affrontare una gamma completa di Security Use Cases

"Vogliamo migliorare la nostra prontezza di risposta agli incidenti".

"Abbiamo bisogno di monitoraggio, indagine e risposta agli incidenti 24 ore su 24, 7 giorni su 7".

"Abbiamo bisogno di supporto per la risposta agli incidenti di emergenza e di un'indagine completa".

"Vogliamo un team pronto ad aiutarci in caso di incidente."

Accesso on-demand a un team di esperti di risposta agli incidenti che bloccherà rapidamente gli attacchi attivi e ti riporterà alle normali operazioni.

- Prezzi scontati sulle tariffe orarie.
- Risposta rapida per ridurre al minimo le interruzioni.
- Può essere utilizzato per i servizi di preparazione agli eventi imprevisti.

SOPHOS

SERVICES

MANAGED SERVICES

- MDR
- Emergency Incident Response
- Vulnerability Management
- Incident Response Retainer

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

PLATFORM

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Cloud

INTEGRATIONS

Broad Ingest
350+ Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

AI-Assisted Workflows and Experiences

SOPHOS X-OPS THREAT INTELLIGENCE

THREAT INTELLIGENCE

- Adversary Tracking
- Threat Research
- Incident and Case Data
- Malware Analysis

AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Early Warning System
- Security Analytics
- Detection Engineering

DATA LAKE

Piattaforma per le operazioni di sicurezza

Acquisizione ampia

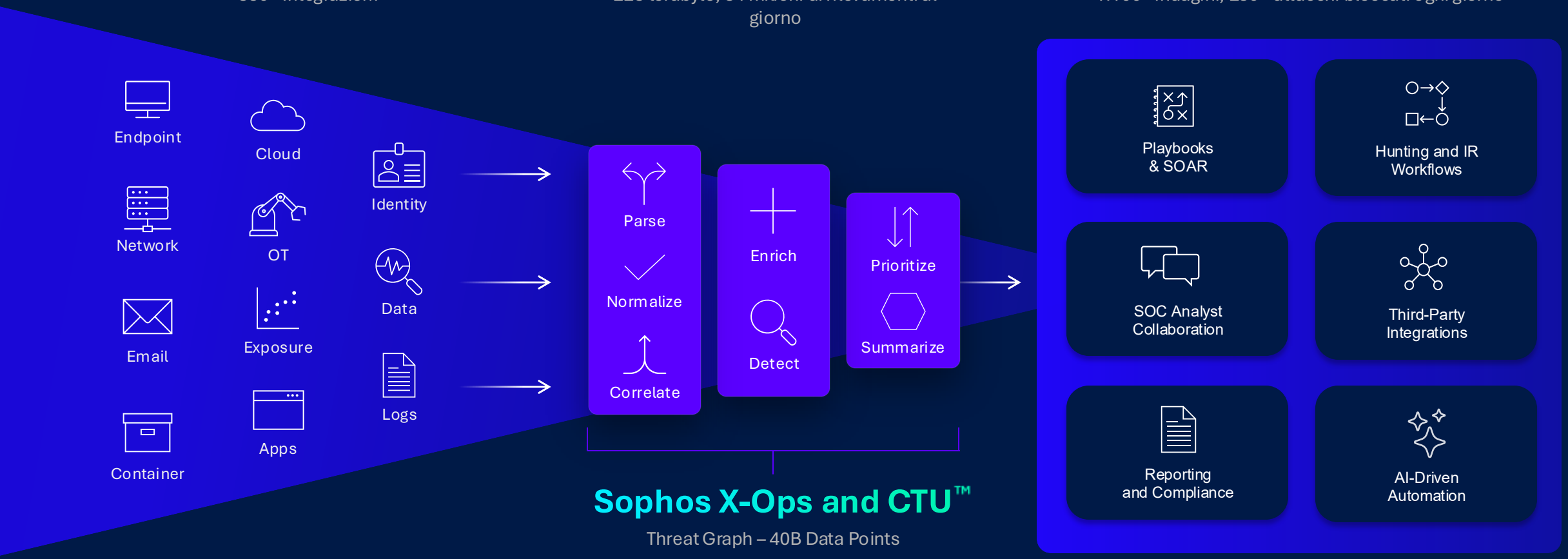
350+ Integrazioni

Rileva e correla

223 terabyte; 34 milioni di rilevamenti al giorno

Indaga e rispondi

1.100+ indagini; 230+ attacchi bloccati ogni giorno



Sophos X-Ops and CTU™

Threat Graph – 40B Data Points

SOPHOS

Usa la tua soluzione di protezione degli endpoint preferita

OPZIONE 1

Sophos Endpoint

SOPHOS

Completamente integrato per una protezione, un rilevamento e una risposta superiori

Incluso automaticamente con Taegis XDR/MDR

OPZIONE 2

Endpoint di terze parti integrato

Microsoft · CROWDSTRIKE · SentinelOne · Carbon Black. by Broadcom

Inserire in modo nativo dati di telemetria e rilevamenti dai provider di endpoint supportati

OPZIONE 3

Altri endpoint di terze parti

paloalto NETWORKS · TREND MICRO · Bitdefender · eset · Trellix · cybereason · BROADCOM · CISCO · FORTINET

-e altro ancora-

Implementa un endpoint di terze parti insieme al nostro sensore "Solo rilevamento"

Alcuni Clienti Taegis

14 of the Fortune 50
31 of the Fortune 100
6 of the Top 20 Financials
5 of the Top 20 Manufactur

Libreria di casi di studio: Cybersecurity Case Study Library |

Cosa rende Sophos Endpoint diverso?

CryptoGuard

BLOCCA IL RANSOMWARE CHE ALTRE SOLUZIONI NON RIESCONO A RILEVARE

- Monitora i file alla ricerca di crittografia dannosa
- Blocca gli attacchi locali e remoti
- Rollback automatico dei file interessati
- Blocca il ransomware remoto
- Non dipende dagli indicatori di "cattivo"
- Protezione MBR (Master Boot Record)

Adaptive Attack Protection

BLOCCA LA PROSSIMA MOSSA DELL'AGGRESSORE PRIMA CHE ACCADA

- Rileva gli attacchi "Hands-on-Keyboard"
- Rafforza dinamicamente le protezioni
- Blocca azioni/comportamenti dannosi
- Impedisce il movimento laterale
- Realizzato dai ricercatori Sophos X-Ops
- Include controlli personalizzabili

Anti-Exploitation

RIDUCI LA SUPERFICIE DI ATTACCO E L'ESPOSIZIONE ALLE MINACCE

- Protezione dagli attacchi zero-day
- Scansione in tempo reale
- Protezione web
- Identificare i dispositivi privi di patch
- Protezione per le applicazioni di Office
- Preconfigurato: non è richiesta alcuna regolazione

Che cos'è un Threat Profile Report?

Prospettiva di rischio esterna generata automaticamente di un potenziale cliente

- **Rapporto rivolto ai clienti - gratuito**

- Prospettiva delle minacce esterne di un ambiente cliente:
  - Domini sospetti registrati
  - Indirizzi e-mail leaked
  - Credenziali esposte in violazioni di terze parti
  - Email dei dirigenti esposte in violazioni di terze parti
  - Vulnerabilità esposte

Combinazione di:

Open-Source Intelligence Information

DNS, Email Records, Public Data Breach Leaks

+

Taegis™ VDR

External Vulnerability Scan

☑ Gratuito ☑ Facile da usare ☑ Report personalizzato

SOPHOS


SOPHOS