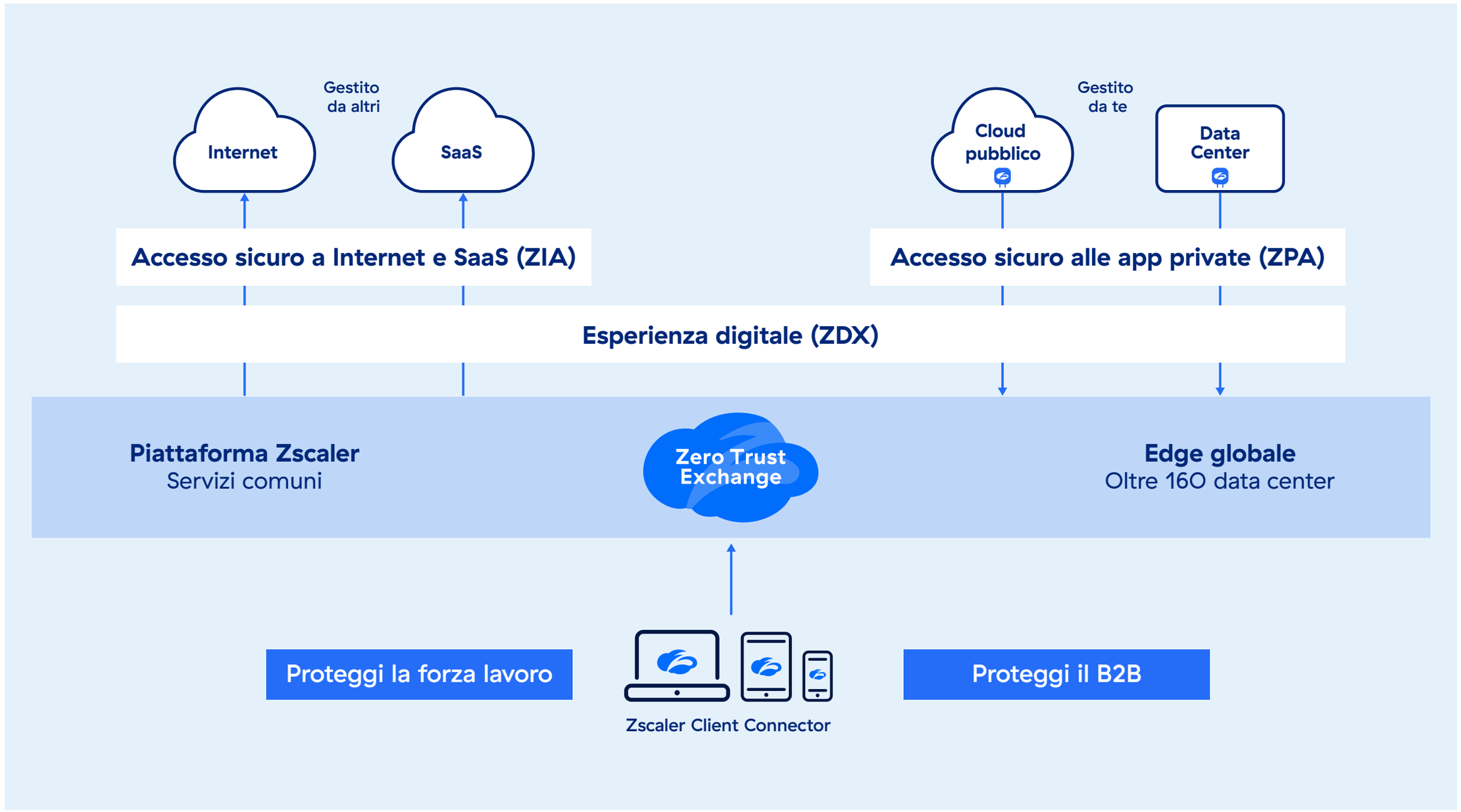
Zscaler Client Connector

Accesso rapido, sicuro e affidabile a qualsiasi destinazione, da qualsiasi luogo o dispositivo.

SCHEDA DATI

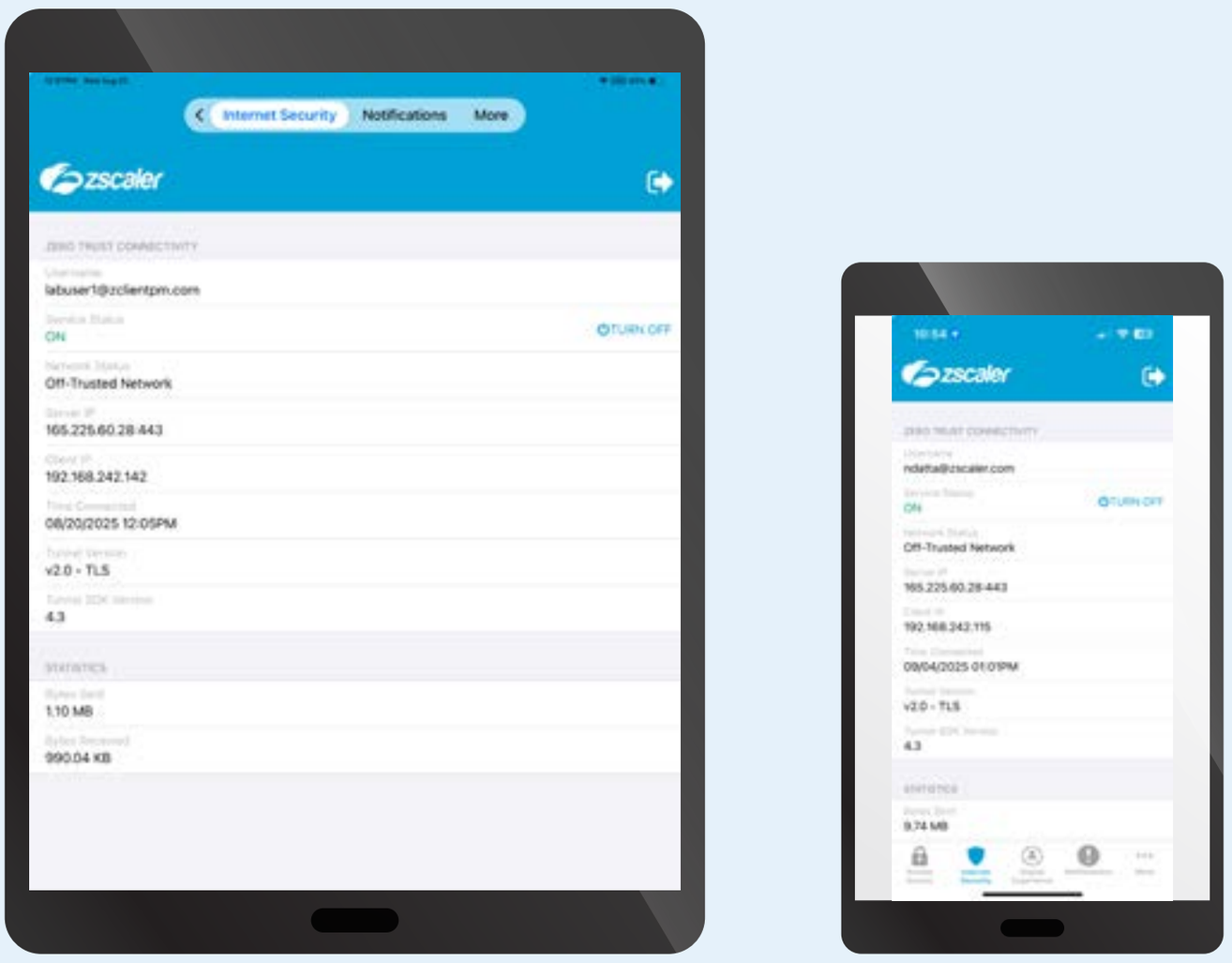


Oggi, i dipendenti lavorano in modo radicalmente diverso rispetto al passato. Ora possono lavorare da qualsiasi luogo e utilizzare un'ampia gamma di dispositivi per accedere ad app cloud e ad altre destinazioni in tutto il mondo. Questa nuova forza lavoro ibrida richiede un accesso rapido e senza interruzioni alle risorse IT, ma ciò non può avvenire a scapito della sicurezza dei dati. Pertanto, qualsiasi organizzazione che voglia avere successo oggi deve proteggere gli endpoint distribuiti a livello globale, garantendo al contempo esperienze utente produttive. Per raggiungere questo obiettivo, innumerevoli team IT si rivolgono a Zscaler e al suo agente per endpoint, Client Connector.

In passato, quando utenti e app si trovavano in ufficio, aveva senso affidarsi a soluzioni di sicurezza e connettività incentrate sulla rete. Ma oggi, i dipendenti fuori sede accedono alle app da remoto tramite reti che i team IT non controllano. Il backhauling di questo traffico verso il data center per proteggerlo aggiunge latenza che compromette la produttività. Ancora più importante, il backhauling intensifica il rischio, in quanto gli utenti vengono collegati alla rete aziendale, il che gli consente di usufruire di autorizzazioni eccessive e di muoversi lateralmente tra le risorse connesse alla rete, senza contare che estende inoltre la superficie di attacco e introduce altri punti deboli critici nella sicurezza.

L’architettura zero trust è la soluzione a tutti questi problemi. Zscaler la fornisce come servizio tramite Zero Trust Exchange, la più grande piattaforma di cloud security al mondo, che funge da centralino intelligente per fornire comunicazioni zero trust any-to-any, utilizzando le policy aziendali invece delle reti. Zero Trust Exchange fornisce l’accesso con privilegi minimi direttamente alle risorse IT in base al contesto, anziché all’indirizzo IP dell’utente, e lo fa all’edge da oltre 160 punti di presenza in tutto il mondo. In altre parole, i team IT possono bloccare le minacce e la perdita dei dati, offrendo al contempo agli utenti esperienze digitali ottimali su qualsiasi dispositivo e ovunque.

Zscaler Client Connector svolge un ruolo centrale nell’offrire comunicazioni zero trust any-to-any. Si tratta dell’agente per endpoint leggero ma multifunzionale di Zscaler, che semplifica l’accesso per gli utenti ovunque siano, rendendolo più efficiente, a privilegi minimi e diretto a Internet e alle risorse IT. Inoltre, fornisce una vasta gamma di altre funzionalità che migliorano ulteriormente la sicurezza e la connettività, eliminando al contempo i prodotti indipendenti e i relativi agenti dedicati.



I vantaggi di Zscaler Client Connector

I vantaggi di Client Connector possono essere più o meno raggruppati nelle sette categorie illustrate di seguito. Per maggiori dettagli, consulta la tabella alla fine di questa scheda tecnica.

Comunicazioni zero trust verso qualsiasi destinazione:
le organizzazioni non devo più ricorrere a soluzioni separate con agenti distinti per proteggere l'accesso a diverse destinazioni. Client Connector fornisce un accesso zero trust con privilegi minimi a qualsiasi destinazione, inclusi web, SaaS e app private, allineandosi con la visione di Gartner su SSE e SASE e garantendo che i dispositivi non vengano rallentati dal sovraccarico causato dagli agenti.

Comunicazioni zero trust per qualsiasi dispositivo:
oltre a proteggere l'accesso a qualsiasi destinazione, le organizzazioni devono proteggere l'accesso su qualsiasi dispositivo, questo perché i dipendenti ora utilizzano un'ampia gamma di dispositivi, tra cui computer desktop, laptop, tablet e smartphone, con una varietà di sistemi operativi differenti. Fortunatamente, Client Connector è in grado di proteggere qualsiasi dispositivo, garantendo la sicurezza e la produttività dei dipendenti.

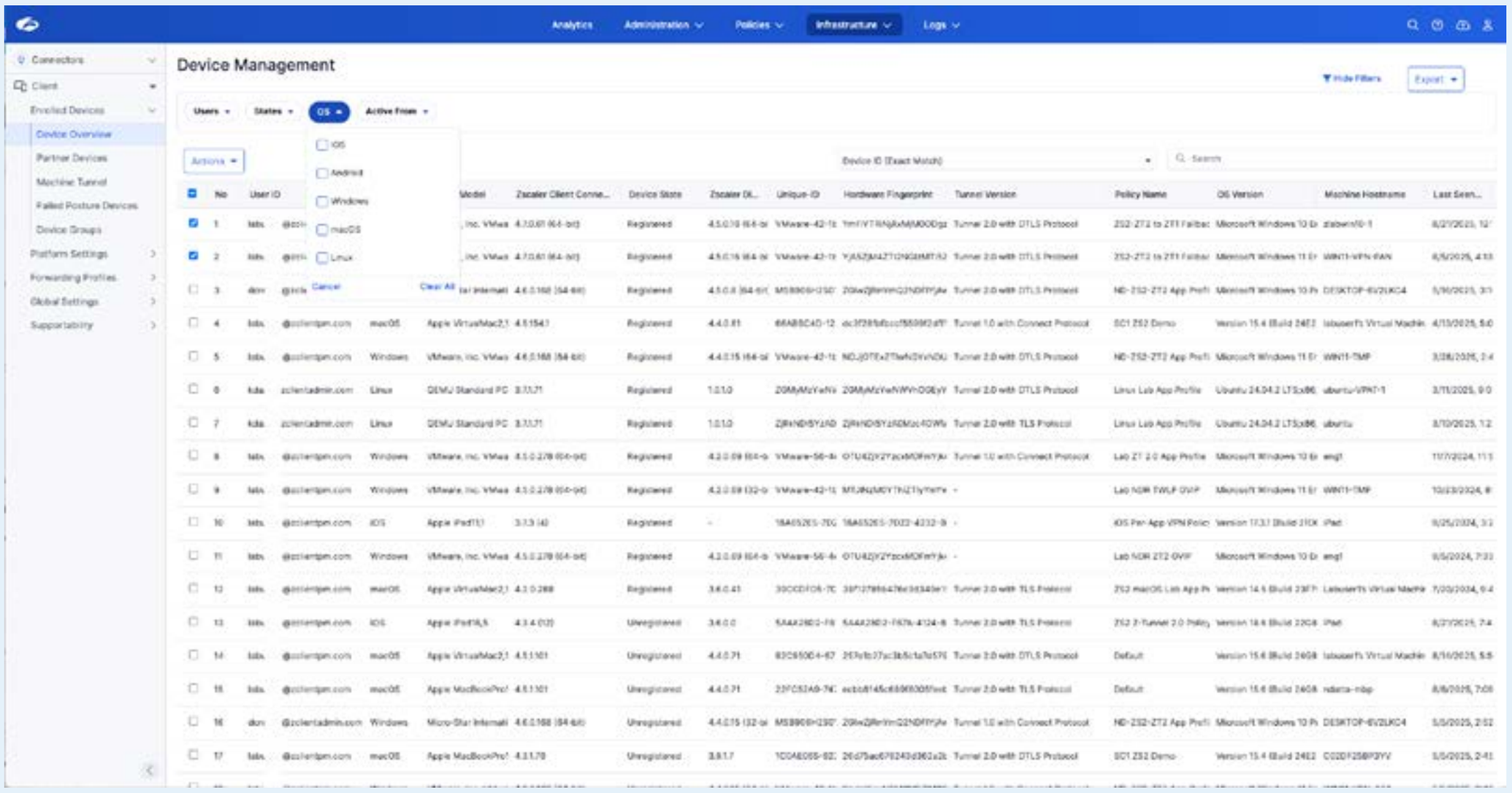
Sicurezza intelligente e basata sul contesto:
l'identità, da sola, non è sufficiente per gestire l'accesso alle risorse IT (le identità possono essere rubate e persino gli utenti legittimi possono ledere inavvertitamente i propri datori di lavoro). Le organizzazioni devono gestire l'accesso in base al contesto e al rischio. Client Connector risponde a questo problema fornendo informazioni sullo stato di sicurezza dei dispositivi che permettono un controllo intelligente e adattivo dell'accesso.

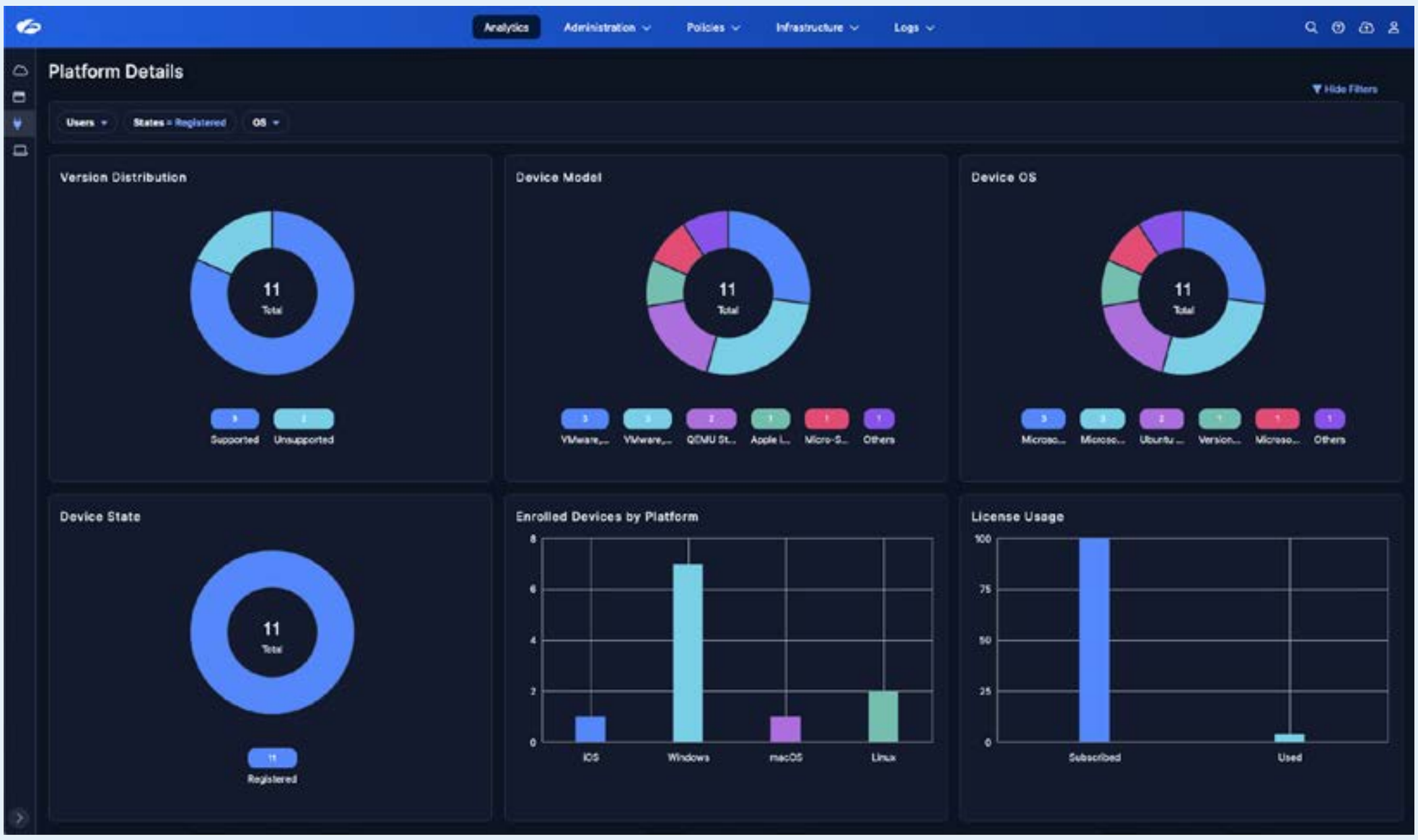
Protezione dei dati sui dispositivi degli utenti finali:
in quanto parte dell'offerta completa di soluzioni per la sicurezza dei dati di Zscaler per proteggere qualsiasi potenziale canale di fuga, Client Connector offre la funzionalità di DLP per endpoint. Grazie a questa funzionalità, le organizzazioni possono proteggere l'archiviazione rimovibile, le condivisioni di rete, la sincronizzazione dell'archiviazione cloud personale e la stampa dagli endpoint, senza dover ricorrere a un altro prodotto da gestire separatamente.

Rilevamento delle minacce nascoste nell'ambiente:
gli aggressori che eludono le difese spesso si nascondono negli ambienti delle organizzazioni per effettuare ricognizioni alla ricerca di pattern dannosi e sfruttabili. Client Connector impiega una tecnologia di deception che sfrutta esche realistiche, come segnalibri, cookie, sessioni e password delle app, per attirare gli aggressori e, una volta effettuato l'accesso alle esche, genera allerte altamente attendibili.

Esperienze utente e produttività superiori:
a differenza degli strumenti legacy che eseguono il backhauling del traffico, Client Connector indirizza il traffico verso la destinazione finale utilizzando il percorso più breve. Offre inoltre a Zscaler Digital Experience (ZDX) la massima visibilità sugli eventi e sullo stato dei dispositivi, che consente agli amministratori di avere un quadro completo della connessione utente, accelerando la risoluzione dei problemi legati all'esperienza utente e migliorando la produttività di utenti e amministratori.

Gestione semplificata e con base cloud:
la gestione di Client Connector tramite l'Experience Center, l'interfaccia utente unificata di Zscaler, consente di ottimizzare l'efficienza operativa, in quanto permette la gestione continua delle policy e del ciclo di vita delle risorse per amministrare l'inoltro e la sicurezza, nonché gli aggiornamenti e i rollback, sfruttando pannelli di controllo e report integrati. Gli amministratori possono inoltre automatizzare le attività tramite OneAPI, un'unica API per l'intera piattaforma Zscaler.





I MODULI DI ZSCALER CLIENT CONNECTOR

Zscaler Internet Access	Basata su un decennio di leadership del Magic Quadrant per il Secure Web Gateway (SWG), ZIA è la soluzione di Zscaler che protegge l'accesso a Internet, applicando al contempo una serie di funzionalità di protezione granulare dalle minacce.
Zscaler Private Access	Zscaler Private Access offre comunicazioni zero trust fluide per tutti gli utenti che accedono alle applicazioni private, sfruttando la segmentazione utente-app guidata dall'IA e policy basate sul contesto che contribuiscono a ridurre i rischi.
Zscaler Digital Experience	Zscaler Digital Experience offre una visibilità end-to-end sulle esperienze utente e consente di rilevare e risolvere rapidamente i problemi prestazionali, migliorando la produttività sia degli amministratori che degli utenti finali.
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) fa parte della soluzione completa Zscaler Data Security e fornisce la visibilità e il controllo necessari sui dati dei dispositivi, riducendo al contempo i costi e la complessità della sicurezza dei dati.
Zscaler Deception	Zscaler Deception distribuisce risorse esca realistiche in tutto l'ambiente IT per attirare gli aggressori nascosti e generare avvisi altamente attendibili che consentono alle organizzazioni di rilevare e bloccare le minacce più rapidamente.

FUNZIONALITÀ E CARATTERISTICHE DI CLIENT CONNECTOR

Supporto completo dei sistemi operativi	**Desktop e thin client:** • Microsoft Windows 11 e Windows 10 su x64 e ARM64 • Apple macOS Tahoe (26), Sequoia (15) e Sonoma (14) su Intel e Apple Silicon • Desktop Linux (RHEL, CentOS, Fedora, Ubuntu, Debian, openSUSE, Arch Linux, Maya OS) • Google Android su ChromeOS • eLux e IGEL OS **Dispositivi mobili:** • Apple iOS 17, 18 e 26 • Google Android 10, 11, 12, 13, 14, 15 e 16
Supporto VDI per utente singolo e multiutente	• Windows 365 Cloud PC, Azure Virtual Desktop • AWS Workspaces • Citrix Virtual Apps & Desktops • Omnissa Horizon e Horizon Cloud Ambienti VDI multisessione supportati con Client Connector for VDI

Ampio supporto per tutti i tipi di traffico	• Tutte le porte e i protocolli (Z-Tunnel 2.0) • Solo traffico web (Z-Tunnel 1.0) • Traffico client-to-client • Traffico server-to-client
Trasferimento tramite tunnel	DTLS 1.2, TLS 1.2 e HTTP CONNECT
Crittografia	• Autenticazione TLS reciproca • Pinning SSL per la connettività del canale di controllo • Conformità FIPS140
Selezione del DC ottimale	Selezione automatica basata su policy: geolocalizzazione, DC preferiti, latenza e destinazione del traffico
Supporto del protocollo Layer 3	IPv4 e IPv6
Metodi di connettività flessibili	• Avviata dall'utente • Su richiesta • Supporto pre-accesso con Machine Tunnels • Sempre attivo • Supporto del profilo VPN aziendale o del profilo VPN per app su iOS • Supporto dual-tunnel (profilo VPN aziendale e VPN per app) su iOS • Supporto del profilo di lavoro per Android
Opzioni per distribuzione e ciclo di vita	• Distribuzione tramite MDM e UEM come Intune, Workspace ONE, JAMF Pro, MobileIron, MaaS360, SCCM e altre soluzioni • Distribuzione tramite Microsoft GPO in Active Directory (AD) • Distribuzioni manuali tramite download diretti da Zscaler • Aggiornamenti delle versioni gestiti dal cloud e supporto per il rollback • Distribuzione rapida di certificati CA root attendibili per l'ispezione SSL • Gestione dei dispositivi e delle policy basata su API
Provisioning degli utenti secondo standard di settore	• Sistema per la gestione delle identità interdominio (SCIM) • Provisioning just-in-time basato su SAML 2.0 • Provisioning just-in-time degli utenti per l'accesso di emergenza • Provisioning automatico dei dispositivi basato sulla chiave della macchina • Provisioning automatico dell'utente/dispositivo basato sul token del dispositivo • Provisioning dei certificati basato su SCEP* • Sincronizzazione di Microsoft AD o LDAP Directory Server • Aggiunta manuale o caricamento in blocco di utenti nel database degli utenti ospitati

Opzioni di autenticazione supportate	• SAML 2.0 • Kerberos • Certificati e smart card • Autenticazione a più fattori (MFA) • Supporto soluzioni token tramite hardware conformi a FIDO2 • Autenticazione del dispositivo basata sulla chiave della macchina per il supporto pre-accesso • Autenticazione utente/dispositivo basata su token • Password • Supporto per l'autenticazione step-up • Autenticazione basata su browser
Piattaforma per il single sign-on	• SSO rapido per Windows • SSO Kerberos • Plug-in Microsoft Enterprise SSO per macOS e iOS • Supporto del Framework Apple Enterprise SSO • Supporto per l'estensione OKTA SSO
Restrizioni utente basate su policy	• Supporto antimanomissione • Restrizioni per OTP e password per controllare la disconnessione dell'utente, l'uscita del client e le restrizioni per l'interruzione del servizio
Lingue supportate	Inglese, francese
Notifiche all'utente finale	**Supporto delle notifiche su desktop e del sistema operativo per:** • Notifiche sulla politica di utilizzo accettabile (AUP) • Stato del servizio • Aggiornamenti software • Autenticazione e ri-autenticazioni periodiche • Eventi di sicurezza dei dati inline • Notifiche e flusso di lavoro di DLP degli endpoint • Notifiche degli eventi relativi alle policy di accesso alle app private e a Internet • Protezione dalle minacce avanzate • Notifiche di sicurezza su Zscaler Zero Trust Firewall, IPS e DNS • Supporto delle notifiche di Zscaler Digital Experience Co-pilot
Strumenti di risoluzione dei problemi integrati	• Recupero automatico dei log cifrati • Esportazioni manuali dei log • Supporto dell'acquisizione automatica e manuale dei pacchetti • Supporto dell'automazione per il monitoraggio e la gestione dei servizi

Supporto esteso del profilo di sicurezza	• Percorso del file • Chiave e valore del registro • Certificato di attendibilità • Certificato del client con CRL • Certificato del client convalidato dal server • Stato del firewall • Crittografia completa del disco • Stato di adesione al dominio AD • Stato di adesione al dominio Entra • Controlli del processo • Rilevamento di Carbon Black in tempo reale • IP di uscita del client • Rilevamento in tempo reale di Microsoft Defender • Rilevamento in tempo reale di CrowdStrike • Punteggio del sistema operativo del dispositivo CrowdStrike ZTA • Punteggio del sensore CrowdStrike ZTA • Rilevamento antivirus • Controlli della versione del sistema operativo • Rilevamento dell'agente JAMF • Livello di rischio JAMF • Modifica non autorizzata • Variabile di proprietà • Versione di Zscaler Client Connector
Altre funzionalità	• Supporto di Disaster Recovery e Business Continuity • Gestione del portale captive incorporato con isolamento opzionale della rete • Gestione del firewall dell'endpoint di Client Connector con blocco della LAN locale • Supporto della quarantena dei dispositivi • Rilevamento e commutazione automatica delle reti attendibili • Supporto degli ambienti No Default Route (NDR)

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

Zero Trust Everywhere