Sophos ZTNA

Zero Trust Network Access

La soluzione che connette in maniera sicura qualunque utente a qualsiasi applicazione, indipendentemente da dove si trovi. Sophos ZTNA connette in maniera trasparente gli utenti ad applicazioni e dati aziendali importanti, offrendo maggiore segmentazione, sicurezza e visibilità rispetto alle VPN di accesso remoto tradizionali. Può essere utilizzato sia come prodotto autonomo che come soluzione completamente integrata di Synchronized Security con Sophos Firewall e Intercept X.

Riacquistare fiducia in un mondo zero trust

Sophos ZTNA concretizza i principi dell'approccio zero trust, il cui motto è "mai fidarsi di niente, meglio controllare tutto". Utenti e dispositivi individuali diventano un perimetro micro-segmentato indipendente, che viene continuamente convalidato e verificato. Gli utenti non si trovano più "all'interno della rete", liberi di usufruire di tutto l'accesso e dell'attendibilità implicita che ne derivano. L'attendibilità viene quindi guadagnata, non regalata.

Abilitazione dell'accesso per i dipendenti in smart working

Sophos ZTNA consente ai dipendenti in smart working di accedere in maniera sicura e trasparente alle applicazioni e ai dati di cui hanno bisogno. Inoltre, facilita i processi di distribuzione, registrazione e gestione, rendendoli molto più semplici rispetto alle VPN tradizionali.

Microsegmentazione delle applicazioni

Sophos ZTNA offre la migliore microsegmentazione in assoluto, permettendo di offrire accesso sicuro alle applicazioni, sia che siano ospitate on-premise, in un data center o nella propria infrastruttura sul cloud pubblico. Inoltre, garantisce visibilità in tempo reale sulle attività delle applicazioni, indicandone stato, condizione di sicurezza e utilizzo. In più, Sophos ZTNA permette di controllare l'accesso a molte applicazioni SaaS, grazie all'uso di restrizioni per gli indirizzi IP, in modo che vengano autorizzate solo le connessioni provenienti dai tuoi gateway ZTNA.

Blocco del ransomware e delle minacce

ZTNA elimina ogni preoccupazione legata alla possibilità che ransomware e altre minacce riescano a propagarsi all'interno della rete dopo aver compromesso il dispositivo di un utente. Utenti e dispositivi hanno solo accesso esplicito e basato sulle policy per applicazioni specifiche. Questo approccio elimina l'attendibilità implicita e la necessità di dover fornire accesso alla rete intera, risolvendo così uno dei principali problemi delle VPN.

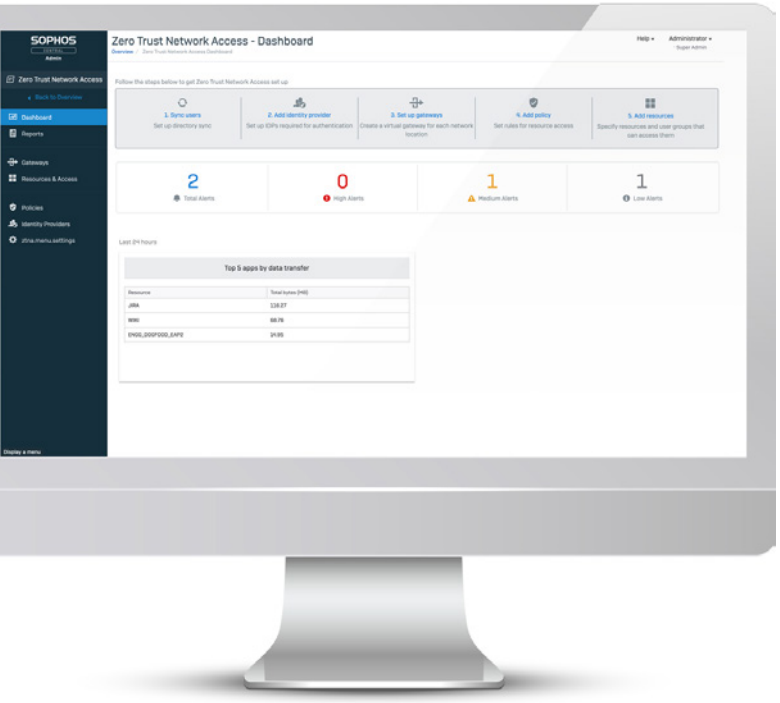
Un sistema rapido da installare, adattare e ridimensionare in base alle esigenze

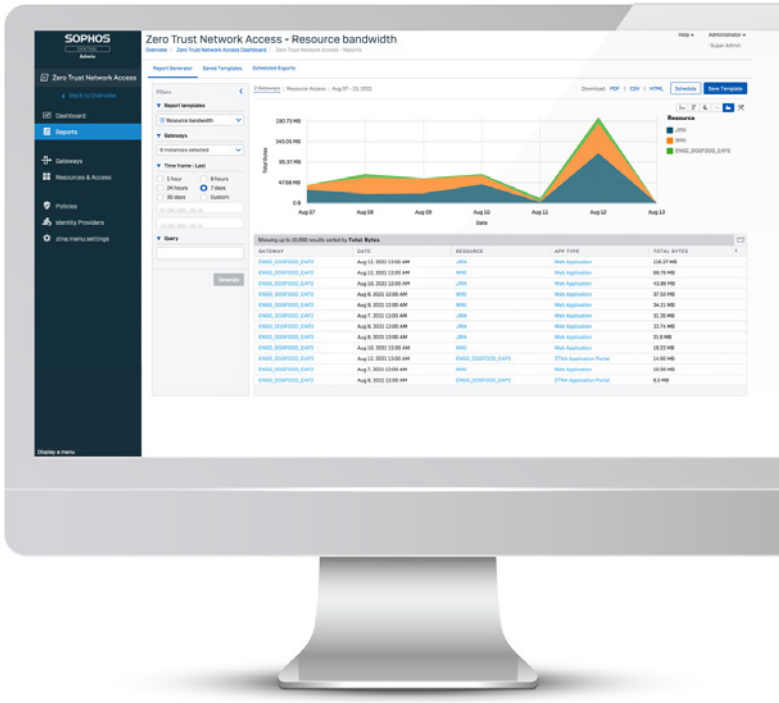
Sophos ZTNA è realizzato per le reti moderne e dalla morfologia dinamica, che crescono velocemente e passano con rapidità al cloud. È una soluzione leggera e pulita che semplifica e riduce i tempi di implementazione rapida e sicura di nuove applicazioni, facilitando anche la registrazione e la rimozione delle autorizzazioni per utenti e dispositivi, nonché la raccolta di maggiori approfondimenti sullo stato e sull'utilizzo delle applicazioni.

Vantaggi principali

- Zero trust: mai fidarsi di niente, meglio controllare tutto
- Integrazione con Sophos Intercept X
- Un unico agent, soluzione basata su una singola console
- La migliore soluzione in assoluto per sostituire le VPN di accesso remoto
- Microsegmentazione e protezione delle applicazioni di rete
- Può essere utilizzato ovunque, sia all'interno che all'esterno della rete
- Gestione e distribuzione dal cloud
- Trasparenza per gli utenti finali
- Visibilità e approfondimenti superiori sulle applicazioni
- Integrazione dello stato di integrità dei dispositivi nelle policy di accesso
- Licenza più semplice, con subscription annuale calcolata in base al numero di utenti e con gateway gratuiti

SOPHOS





Distribuzione e gestione dal cloud

Sophos ZTNA è stato concepito e progettato per semplificare l'implementazione del sistema Zero Trust Network Access e renderlo integrato e sicuro. Sophos ZTNA viene distribuito e gestito dal cloud, ed è integrato in Sophos Central: la scelta numero uno tra le piattaforme cloud di cybersecurity con funzionalità di gestione e reportistica.

Da Sophos Central è possibile non solo gestire ZTNA, ma anche i Sophos Firewall e altri prodotti di protezione per endpoint, server, dispositivi mobili, cloud, e-mail e molto di più. Basta accedere per gestire l'intera struttura di IT security da qualsiasi luogo, a qualsiasi ora e su qualsiasi dispositivo.

Un unico agent, un'unica console, un unico vendor

Sophos ZTNA offre un'integrazione insuperabile con l'intero ecosistema di cybersecurity Sophos, per semplificare notevolmente il lavoro dei responsabili IT. Prevede un unico agent per ZTNA e protezione endpoint next-gen. Inoltre, viene gestito da una singola console di gestione in Sophos Central, per approfondimenti di livelli precedentemente impensabili su tutti i prodotti di IT security.

I clienti concordano: implementare una soluzione di cybersecurity Sophos completamente integrata comporta notevoli vantaggi in termini di risparmio di tempo. Sostengono che equivale a raddoppiare il numero di dipendenti nel proprio reparto IT.

Un'integrazione insuperabile: ZTNA E Protezione Endpoint Next-Gen

Sophos ZTNA è l'unica soluzione ZTNA strettamente integrata con un prodotto di protezione endpoint next-gen: Sophos Intercept X. Questa combinazione implica enormi vantaggi in termini di protezione, distribuzione e gestione.

- Protezione end-to-end: accesso sicuro alle applicazioni e protezione di endpoint e reti contro violazioni e minacce come il ransomware, grazie alle più potenti tecnologie di machine learning e sicurezza endpoint next-gen disponibili sul mercato.
- Synchronized Security: l'integrazione tra ZTNA ed endpoint permette la condivisione costante di informazioni relative a stato e integrità, per isolare i sistemi compromessi e impedire così che le minacce trasferiscano dati o prelevino illecitamente informazioni.
- La praticità di un unico agent, un'unica console, un unico vendor.

È una combinazione vincente che nessun altro vendor può offrire.

Distribuzione con un unico agent

Sophos ZTNA prevede un'integrazione profonda con la sicurezza endpoint next-gen di Sophos Intercept X, e questa caratteristica consente di distribuire la soluzione con un unico client.

Questo tipo di infrastruttura include la migliore protezione endpoint antiransomware disponibile sul mercato, più la soluzione più efficace in assoluto per la segmentazione e la sicurezza delle applicazioni. Tutto con una distribuzione a client singolo.

È anche disponibile un'opzione con accesso indipendente dal client per le applicazioni basate sul browser.

Gateway delle applicazioni scalabili

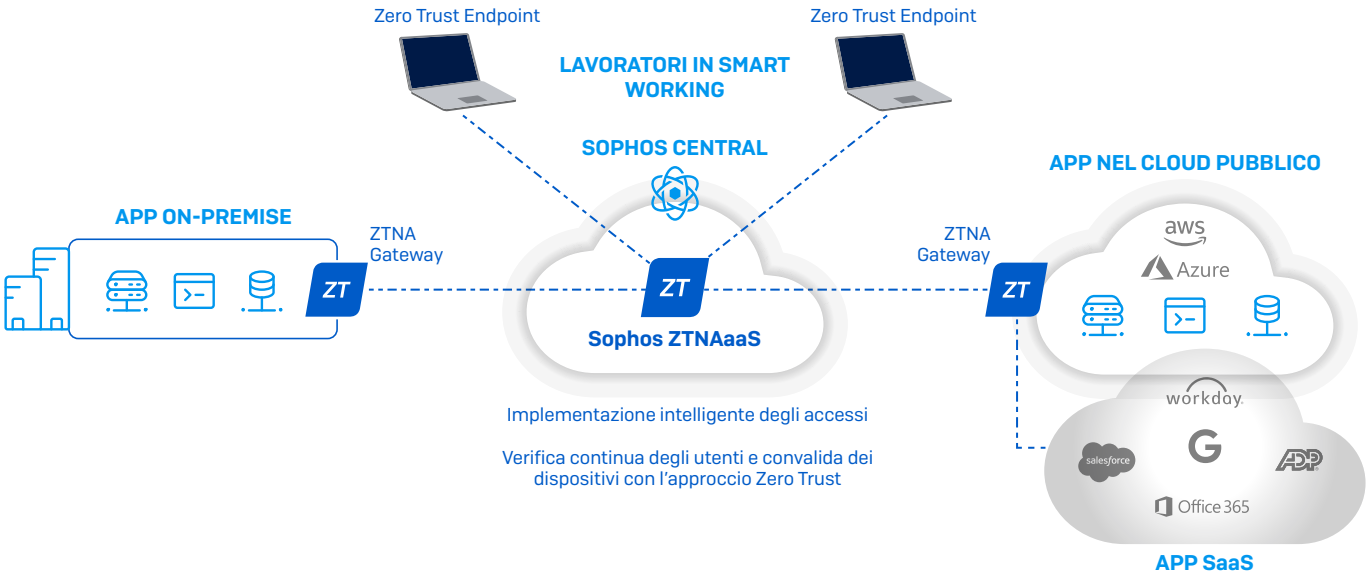
I gateway Sophos ZTNA sono gratuiti e facili da distribuire dove richiesto. Sono disponibili come appliance virtuali e possono essere distribuiti come gateway con disponibilità elevata, per una struttura scalabile, che può essere estesa in base alla crescita dell'organizzazione.

Integrità sincronizzata del dispositivo

Sophos ZTNA sfrutta tutti i vantaggi della Sophos Synchronized Security utilizzando il Security Heartbeat™ tra gli endpoint con Sophos Intercept X e Sophos Central: questa tecnologia permette a ZTNA di valutare lo stato di integrità del dispositivo e di identificare eventuali minacce attive e indicatori di compromissione. Il risultato è una soluzione che avvia una risposta immediata per limitare l'accesso (sia all'interno che all'esterno della rete) per i dispositivi compromessi o non conformi alle policy.

Identità integrata

Con zero trust, l'identità è tutto. Sophos ZTNA verifica continuamente l'identità degli utenti, grazie al supporto dei più comuni provider di identità (Identity Provider, IDP), inclusi Microsoft Azure e Okta. Naturalmente è anche possibile implementare una soluzione di autenticazione a fattori multipli (Multi-Factor Authentication, MFA) a scelta, compatibile con questi IDP, per proteggere i sistemi dai tentativi di furto di credenziali e dai dispositivi compromessi.



Sophos Zero Trust Endpoint

La soluzione può essere eseguita in modalità agentless, oppure con l'agent Sophos ZTNA a impatto minimo, che si integra con Sophos Intercept X per offrire la soluzione endpoint Zero Trust definitiva, con Synchronized Security. Se preferisci, Sophos ZTNA è anche compatibile con il tuo prodotto di protezione endpoint attuale.

Sophos Central

Semplifica l'uso di ZTNA as a Service, grazie alla rapidità di distribuzione, ai controlli granulari delle policy e a ottime opzioni di visibilità e reportistica sul cloud. Si integra con i principali provider di identità, per abilitare l'implementazione intelligente degli accessi alle tue applicazioni, grazie alla verifica continua degli utenti e alla convalida dei dispositivi.

Gateway Sophos ZTNA

Disponibile su Hyper-V, VMware e Amazon Web Services come appliance virtuale gratuita e semplice da installare. Rende le tue applicazioni invisibili all'Internet pubblico e garantisce una connessione sicura per gli utenti verificati e i dispositivi convalidati, in modo che possano accedere alle applicazioni di cui hanno bisogno per svolgere il proprio lavoro.

Riepilogo delle funzionalità di Sophos ZTNA

- Accesso protetto: per applicazioni ospitate on-premise o nella propria infrastruttura sul cloud pubblico
- Applicazioni: tutte le app web basate sul browser in modalità indipendente dal client; app thick client come SSH, VNC, RDP e altre, tramite il client ZTNA
- Policy di accesso: policy per gli utenti basate sui gruppi, policy di accesso di Synchronized Security basate sull'integrità
- Reportistica, monitoraggio, log e controllo di stato, accesso e utilizzo delle applicazioni tramite Sophos Central
- Portale utenti per permettere agli utenti finali di accedere alle applicazioni aggiunte ai segnalibri

Specifiche tecniche

Piattaforme supportate	Attualmente	In programma
Provider di identità	Microsoft Azure e Okta	Provider di identità aggiuntivi, a seconda della richiesta
Piattaforme ZTNA Gateway	VMware ESXi 6.5+, Hyper-V 2016+ e AWS	Azure, Nutanix e GCP
Piattaforme ZTNA Client	Windows 10 1803 o versioni successive, macOS 11 (Big Sur) o versioni successive	iOS e Android
Stato di integrità del dispositivo ZTNA	Sophos Security Heartbeat (Intercept X)	È in programma l'inclusione degli attributi di valutazione dello stato del Centro sicurezza Windows

Specifiche per il gateway	
VM consigliata	2 Core/4GB
Cluster a più nodi	Fino a 9 nodi con bilanciamento del carico per garantire performance, capacità e continuità aziendale
Capacità e scalabilità dei nodi	10.000 connessioni agent per un singolo nodo, fino a 90.000 connessioni agent in un cluster (max 9 nodi)

Informazioni Sull'Acquisto

La licenza Sophos ZTNA viene calcolata come subscription annuale in base al numero di utenti. I gateway ZTNA possono essere distribuiti gratuitamente, nella quantità richiesta.

Per maggiori informazioni, visitare:
sophos.it/ztna

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

23-01-10 DS-IT (DD)

SOPHOS