

Seqrite ZTNA

SECURITE



Metti in sicurezza l'accesso degli utenti alle applicazioni aziendali in un ambiente di lavoro senza confini fisici.

www.seqrite.com





Perché le aziende dovrebbero garantire ai dipendenti accessi sicuri alle risorse aziendali anche oltre i confini fisici dell'azienda?

Al giorno d'oggi il ricorso delle aziende al lavoro remoto, così come al cloud, si è fatto massivo. Questo ha comportato una novità che ha rivoluzionato il concetto di sicurezza informatica aziendale: il perimetro dell'azienda, le 4 mura, la sede fisica non sono più confini effettivi. I dipendenti da remoto sono a casa, presso la sede di un cliente, in giro per il mondo... ovunque siano, i dipendenti remoti fanno perdere senso ai confini aziendali tradizionali mentre l'azienda sperimenta l'evidenza che i dati e le risorse aziendali sono anche fuori dalle 4 mura. Le aziende di oggi devono ormai ragionare in termini di confini virtuali, dovendo proteggere tutte le risorse aziendali, ovunque esse si trovino.

In questo contesto, la protezione dei dati sensibili e riservati dell'azienda è messa costantemente a repentaglio da minacce nuove e avanzate: per i team di sicurezza la protezione dei moderni ambienti di lavoro ibridi rappresenta una grande sfida.

Le misure di sicurezza convenzionali come le VPN e i perimetri aziendali sono inadeguate alle esigenze di condivisione e flessibilità della forza lavoro attuale. L'uso dei dispositivi personali a fini lavorativi e altri dispositivi non gestiti introducono nuovi rischi e vulnerabilità, mentre i dati aziendali finiscono dispersi tra più piattaforme.

I privilegi di accesso, in questo quadro, rappresentano un vettore di minaccia molto pericoloso rendendo così necessaria l'adozione di un modello di sicurezza informatica in linea con un ambiente di lavoro ibrido verificando costantemente accessi, utenti, dispositivi.





A₁

A₁

Presentazione di Seqrite ZTNA

Seqrite ZTNA è una soluzione SaaS per l'accesso Zero Trust alla rete aziendale: fornisce un accesso remoto sicuro alle applicazioni e ai servizi aziendali per dipendenti, collaboratori esterni e fornitori in un ambiente di lavoro ibrido senza confini fisici.



Approccio **Zero Trust** Sicurezza per un nuovo mondo!

01 **Implementa Zero Trust Network Access di Seqrite per l'accesso sicuro al tuo ambiente di lavoro ibrido**

Implementa un approccio Zero Trust per la tua azienda e applicalo a qualsiasi dipendente, fornitore, partner ecc... garantendo un accesso sicuro ai tuoi sistemi e applicazioni indipendentemente che siano entro o fuori la rete aziendale. Seqrite ZTNA utilizza policy declinate in base al contesto, processi e un approccio tecnologico capace di bloccare accessi non autorizzati.

02 **Adotta il modello Zero Trust**

Autentica ogni tentativo di accesso effettuato da dipendenti, fornitori e altri partner. Applica impostazioni basate sugli attributi degli utenti, i dispositivi, le posizioni, i dettagli di rete e altri identificatori prima di concedere l'accesso alle applicazioni aziendali.

03 **Applica il principio del Privilegio Minimo**

Applica il principio del Privilegio Minimo, che si adatta perfettamente al mondo del lavoro iper flessibile di oggi: fornisci agli utenti autenticati l'accesso solo a determinate applicazioni e con il minor numero possibile di privilegi.

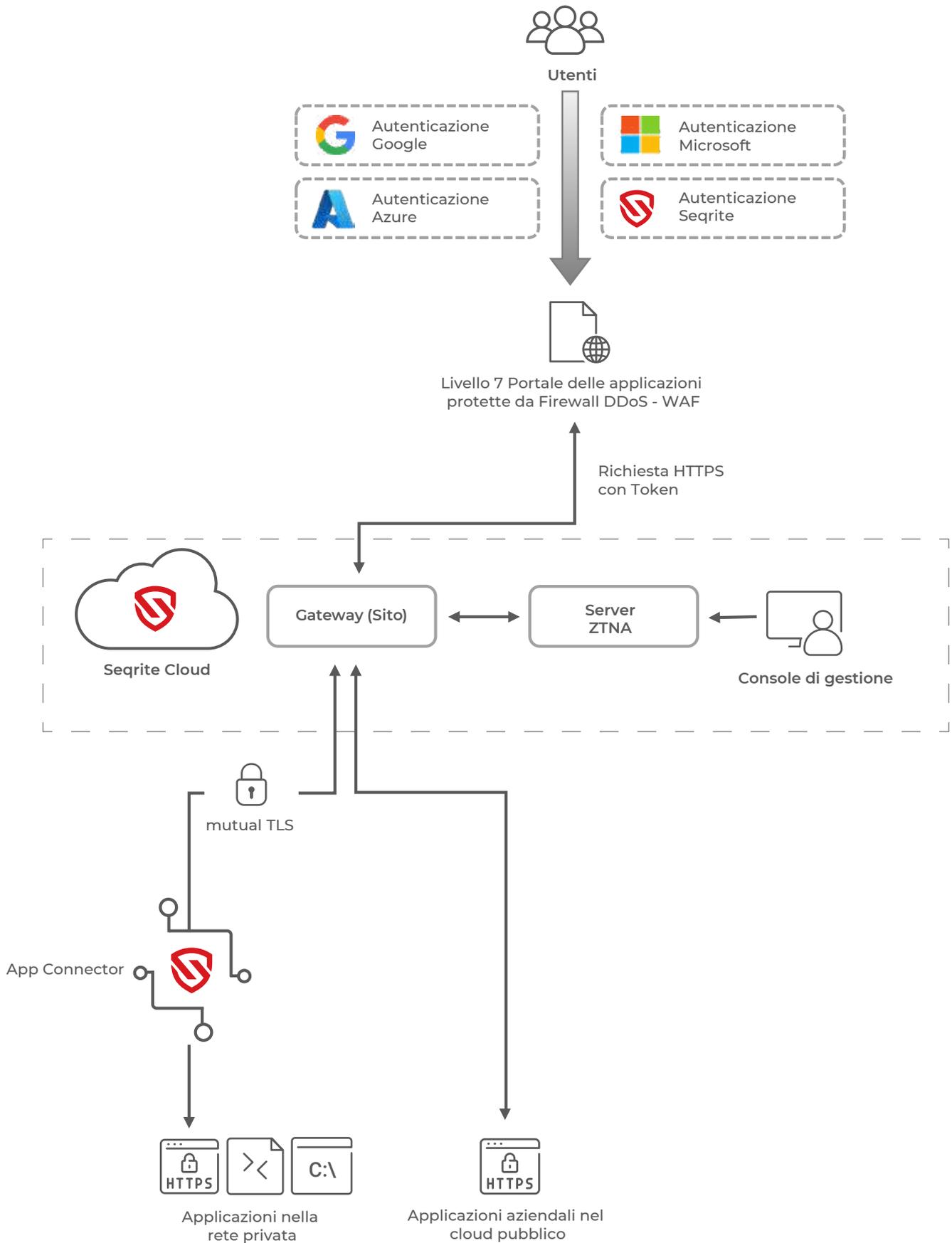
04 **Stabilisci una postura di sicurezza Integrata**

Si integra perfettamente con le soluzioni di sicurezza già presenti, per rafforzare in modo efficiente la postura di sicurezza integrata della tua azienda. I clienti che già hanno adottato la piattaforma Seqrite CSM (quindi Data Privacy, XDR e EPP Cloud) potranno utilizzare Seqrite ZTNA per fornire un accesso sicuro alle applicazioni aziendali.





Come funziona ZTNA





Perché la tua azienda ha bisogno di Seqrite ZTNA?

Procedura di inserimento semplice e veloce:

- Pronto in pochi minuti.
- Inizia con pochi utenti e applicazioni e poi espandi gradualmente.
- Integrazione semplice con l'infrastruttura IT esistente per la gestione delle identità.

Visibilità totale sugli accessi Zero Trust per gli amministratori:

- Riepiloghi grafici di come gli utenti accedono alle app aziendali.

Semplificazione delle policy di gestione

- Utilizza tag aziendali o etichette applicabili agli utenti e alle applicazioni per definire politiche che semplificano i processi di cambio degli utenti nella tua azienda.

Più efficienza per la tua azienda:

- Migliora le prestazioni senza costi aggiuntivi.
- Elimina gradualmente il MPLS (Multi-protocol Label Switching) e passa alle applicazioni tramite Internet: avrai una soluzione economica senza sacrificare le prestazioni.

Ridurre la complessità e migliorare la sicurezza:

- Semplifica l'infrastruttura tecnologia e riduci al minimo il debito tecnico adottando un modello di accesso sicuro incentrato sull'utente e sull'applicazione.
- Tramite questa soluzione innovativa, è possibile semplificare i processi, ridurre la complessità e migliorare la sicurezza riducendo al minimo i costi.





Aspetti chiave del prodotto



Gestione dell'identità:

- Integrale con il tuo cloud idPs come Google Workspace o Microsoft Azure.
- Connettilo con il Server Active Directory 2012/16/19/ADFS o gestione locale degli utenti tramite Seqrite Centralized Security Management.
- Autenticazione basata sugli OTP per il database utenti locale.



Accesso alle applicazioni

- Opzioni di accesso con o senza agent per le applicazioni con protocollo: HTTPS, HTTP, RDP, SSH, Telnet, VNC, FTP, SMB ecc...
- Autenticazione sicura delle applicazioni e accesso a Office 365 e alle applicazioni di Google Workspace.
- Accesso continuo alle applicazioni e ai servizi critici per gli utenti aziendali, senza esporre la rete o l'applicazione al mondo esterno.



Politiche Zero Trust

- La policy Zero Trust definisce quale utente(i) ha accesso a quale app con un approccio che, di default, è orientato a negare l'accesso.
- Layer 7 Firewall Policy per bloccare il traffico originato da IP/paesi indesiderati e consente solo il traffico necessario.
- Layer 7 DDoS Policy per consentire solo un certo numero di richieste entro un dato lasso di tempo, rigettando il resto.
- La verifica della postura di sicurezza dei dispositivi si basa su più fattori per garantire l'accesso ai dispositivi corretti.



Controllo granulare sulle applicazioni

- Possibilità di limitare le sessioni desktop da remoto ad un'applicazione o concedere l'accesso alle applicazioni da remoto invece di esporre l'intero server.
- Applica restrizioni per gli accessi agli appunti e al trasferimento di file.
- Visualizza le attività dell'utente attraverso la registrazione della sessione.
- Regole WAF (Web Application Firewall) per proteggere le applicazioni aziendali critiche da attacchi contro il livello 7 come SQL injection, cross site scripting, OS command Injection ecc....



Modelli di licenza per Seqrite ZTNA

Nome prodotto	TRIAL EDITION 30-giorni	STANDARD EDITION 1-3 anni	ENTERPRISE EDITION 1-3 anni
Descrizione	Prova gratuitamente per 30 giorni l'accesso sicuro da remoto. Connetti i tuoi dipendenti, applicazioni e servizi.	Accesso da remoto sicuro per piccole e medie imprese	Accesso da remoto sicuro per grandi imprese
Prezzo	Gratuito per 30 giorni	Abbonamento annuale €	Abbonamento annuale €
Accesso da remoto			
Portale di amministrazione in cloud	SI	SI	SI
Numero di siti	1 sito	1 sito	1 sito
Numero di gruppi	1 gruppo	Up	Unlimited
Supporto accesso da remoto sicuro basato su agenti e senza agenti	SI	SI	SI
Configurazioni:			
Identity Provider supportati	Gli IdPs supportati sono: AD 2012 - 2016 - 2019 (LDAP) ADFS (SAML) Microsoft Azure AD (SAML) Google Workspace (SAML)	Gli IdPs supportati sono: AD 2012 - 2016 - 2019 (LDAP) ADFS (SAML) Microsoft Azure AD (SAML) Google Workspace (SAML)	Gli IdPs supportati sono: AD 2012 - 2016 - 2019 (LDAP) ADFS (SAML) Microsoft Azure AD (SAML) Google Workspace (SAML)
Supporto ai domini personalizzati	SI Richiede la verifica DNS dal lato del cliente	SI Richiede la verifica DNS dal lato del cliente	SI Richiede la verifica DNS dal lato del cliente
Numero di applicazioni e servizi	Fino a 10 applicazioni e servizi	Fino a 100 applicazioni e servizi	Illimitato
Supporta le registrazioni di sessioni per WebRDP, WebSSH, WebTelnet & WebVNC	NO	Add-on	Add-on
Numero di utenti per il portale Cloud (dipendenti, appaltatori e fornitori)	Fino a 10 utenti	Fino a 1000 utenti	Illimitato
Numero di Endpoint con agent Seqrite ZTNA	Fino a 30 utenti	Fino a 500 utenti	Illimitato
Conservazione dei Log:			
Numero di giorni di conservazione dei log sul cloud, i sistemi e le applicazioni	Superiore ai 30 giorni	Superiore ai 180 giorni	Superiore ai 180 giorni
Numero di giorni per i quali verrà conservato l'Audit Trail	Superiore ai 30 giorni	Superiore ai 180 giorni	Superiore ai 180 giorni



Info su Seqrite

Seqrite è un fornitore leader di soluzioni di cyber security aziendale. Avendo a mente, come primo obiettivo, quello di semplificare la sicurezza informatica e renderla accessibile alle PMI, Seqrite offre soluzioni e servizi completi mettendo a disposizione dei clienti tecnologie brevettate e i vantaggi dell'Intelligenza Artificiale (AI) e del Machine Learning (ML). Le soluzioni di sicurezza di Seqrite proteggono le aziende dalle minacce più avanzate grazie a più livelli di sicurezza posti a difesa di dispositivi, applicazioni, reti, cloud e dati. Seqrite è il ramo di sicurezza informatica per le aziende di Quick Heal Technologies Limited, l'unica società di prodotti e soluzioni di cybersecurity quotata in borsa in India.

Oggi, oltre 30.000 imprese in più di 76 Paesi si affidano a Seqrite per le loro esigenze di cybersecurity.

SEQRITE

Quick Heal Technologies Limited

Seqrite Italia www.seqrite.it | cs@s-mart.biz | +39 055 43 03 52 | Distribuito da s-mart.biz 

Tutte le Proprietà Intellettuai, compreso Marchio/i di Fabbrica, Logo/i, Copyright sono di proprietà dei rispettivi proprietari. Copyright©2024 Quick Heal Technologies Ltd. Tutti i diritti riservati