ZYXEL
NETWORKS

Sicurezza di rete senza complicazioni



Settembre 2026

La cybersecurity, resa semplice

Ogni piccola impresa merita una sicurezza di rete affidabile e facile da gestire. È il principio alla base di tutto ciò che facciamo in Zyxel Networks ed è lo stesso approccio che oggi applichiamo alla cybersecurity.

Abbiamo costruito la nostra reputazione rendendo la tecnologia di networking accessibile alle PMI e oggi applichiamo la stessa filosofia alla loro sicurezza. Siamo conosciuti soprattutto per le nostre soluzioni di switching e WiFi, ma abbiamo anche una lunga esperienza nella cybersecurity, supportata dalla nostra rete globale di sicurezza e da collaborazioni consolidate con i principali fornitori del settore.

In questo documento spieghiamo come rendiamo la sicurezza più semplice, cosa distingue il nostro approccio e la nostra proposta di valore e perché tutto questo è importante per installatori, integratori e MSP che lavorano con le piccole imprese.



Il panorama delle minacce è cambiato. La protezione deve stare al passo.

La sicurezza digitale è molto diversa da quella dei primi anni di internet, quando uno dei principali consigli era semplicemente scegliere una password sicura.

Negli ultimi 40 anni, le minacce che le aziende devono affrontare sono aumentate e si sono evolute: dai tentativi di accesso non autorizzato e dai malware fino a tecniche sempre più sofisticate e ingannevoli, come phishing e ransomware.

Con l'evoluzione delle minacce è cresciuta anche la protezione necessaria per contrastarle, e la cybersecurity è diventata un settore sempre più specializzato e complesso.

La complessità è reale. Ma non deve ricadere interamente sulle piccole imprese.

Protezione completa, senza complicazioni

Crediamo che la risposta a un panorama di minacce sempre più complesso non sia aggiungere altra complessità per il cliente, ma integrare in modo intelligente le diverse forme di protezione.

Riunendo in un'unica soluzione la protezione contro un'ampia gamma di minacce, possiamo offrire ai clienti finali una protezione completa che riduce in modo significativo il rischio, senza chiedere loro di diventare esperti di sicurezza.

È esattamente ciò che abbiamo fatto con la serie di firewall USG FLEX H, che integra tecnologie di protezione dei principali specialisti della sicurezza.

Insieme alla nostra dashboard, agli strumenti di reportistica SecuReporter e alla piattaforma di gestione cloud Nebula, offriamo una soluzione completa che permette a PMI, professionisti e lavoratori da remoto di avere la protezione di cui hanno bisogno a un costo accessibile. E, allo stesso tempo, consente di verificare con chiarezza l'efficacia della protezione e di configurare e gestire la sicurezza da remoto.



Rendere la sicurezza più accessibile per le piccole imprese

Oltre a percepire la cybersecurity come complessa, molte PMI semplicemente non hanno il tempo per capire di cosa hanno bisogno. Le aziende più piccole, inoltre, spesso non hanno personale IT dedicato né competenze interne specifiche sulla sicurezza digitale. Anche trovare e mantenere in azienda persone con le competenze giuste può essere difficile.

Anche il budget è un fattore concreto: il costo dei dispositivi e dei rinnovi delle licenze pesa soprattutto sulle aziende con risorse limitate.

È proprio per questo che lavoriamo per rendere le nostre soluzioni accessibili e facili da giustificare, così che la mancanza di competenze interne o un budget limitato non significhino dover rinunciare alla protezione.



Perché la protezione è importante

Quando le piccole imprese adottano le giuste misure di sicurezza, riducono in modo significativo il rischio di subire un attacco informatico. Secondo il 2026 SMB Cyber Readiness Index di ESET, il 64% delle organizzazioni EMEA intervistate prevede di subire un attacco informatico nel prossimo anno, mentre il 44% ha subito un incidente di cybersecurity negli ultimi 12 mesi. I dati mostrano che gli attacchi sono una realtà concreta per aziende di ogni dimensione e che prepararsi adeguatamente fa la differenza.

Il livello di protezione deve essere proporzionato alle esigenze dell'azienda e al suo livello di rischio. Un'azienda che gestisce dati finanziari personali, ad esempio, può avere informazioni più sensibili rispetto a un bar o a un parrucchiere. Ma ogni azienda conserva dati che vale la pena proteggere, dai dati bancari alle informazioni personali di clienti e dipendenti.

44% **delle organizzazioni EMEA ha subito un incidente di cybersecurity negli ultimi 12 mesi**



Cosa devono proteggere le PMI

Proteggere il punto di accesso alla rete, cioè la connessione a internet dove si trova il firewall, è un ottimo punto di partenza.

Ma non basta. Tutti i dispositivi connessi dovrebbero avere una forma di protezione ed essere mantenuti aggiornati. Idealmente, l'attività di rete dovrebbe essere registrata e analizzata con regolarità. È inoltre utile avere una policy di sicurezza e fare in modo che i dipendenti sappiano riconoscere e gestire email e link sospetti.

Queste misure non servono solo a ridurre il rischio. Creano una base solida e concreta per proteggere sistemi e dati aziendali.
La maggior parte delle aziende preferirà comunque affidarsi a un partner che si occupi ogni giorno di aggiornare licenze e firmware, monitorare la rete e verificare lo stato della sicurezza. È qui che entrano in gioco installatori, integratori e MSP.

Una vera opportunità per IT e installatori tecnici

Molte PMI configurano in autonomia laptop, PC e reti WiFi di base oppure si affidano a uno specialista IT locale. Per la videosorveglianza, la sicurezza fisica, gli allarmi antincendio e tecnologie smart come i sistemi di controllo degli accessi, invece, si rivolgono in genere a installatori specializzati.

Per queste piccole società di consulenza IT e aziende di installazione, la cybersecurity rappresenta quindi una vera opportunità: un nuovo flusso di ricavi da sviluppare.

La complessità ha comprensibilmente frenato alcuni partner in passato. Nessuno vuole mettere a rischio una relazione di fiducia con il cliente. Il nostro approccio semplice alla sicurezza aiuta a superare questa barriera.

Con la serie USG FLEX H, gli installatori possono offrire ai clienti tutta la protezione di cui hanno bisogno, con un unico dispositivo. Un processo di configurazione in cinque passaggi, effettuato prima della consegna, rende più semplice preparare e installare il firewall, mentre le impostazioni predefinite sono pensate per adattarsi alla maggior parte delle piccole imprese senza bisogno di modifiche.

Un'installazione semplice che fa davvero la differenza

La semplicità di installazione fa la differenza: permette a tutti di risparmiare tempo, lavoro e costi. Il cliente non deve aspettare la visita di un tecnico per completare la configurazione: una volta collegato, il firewall si configura automaticamente.

I partner non devono diventare specialisti di cybersecurity per offrire la soluzione. E, per chi vuole andare oltre, un partner IT o un installatore può utilizzare facilmente la piattaforma cloud Nebula per monitorare i dispositivi dei clienti e apportare modifiche da remoto.

Una volta installato, con licenze di sicurezza e firmware mantenuti aggiornati, il firewall continua a offrire una protezione completa con un intervento minimo o nullo da parte del partner.

E quando serve assistenza, il team Zyxel Networks è sempre a disposizione con supporto e assistenza personalizzati in italiano.



Serie di firewall USG FLEX H: caratteristiche e vantaggi principali

La serie Zyxel USG FLEX H è progettata per soddisfare le esigenze di piccole imprese di ogni dimensione e con budget diversi. Ogni modello include di serie l'intero set di funzionalità di sicurezza: anche il modello più compatto ed economico offre una protezione completa. La principale differenza tra i modelli riguarda velocità e capacità. I modelli di fascia più alta sono pensati per aziende con un numero maggiore di utenti e maggiori esigenze di throughput.

Cosa è incluso

Tutte queste funzionalità e caratteristiche sono incluse di serie in ogni modello della serie USG FLEX H:

- **Rilevamento delle minacce basato sull'AI:** analizza in tempo reale l'intelligence globale sulle minacce per identificare e rispondere ad attacchi informatici in evoluzione e sempre più sofisticati
- **Sandboxing cloud:** isola i file sconosciuti o sospetti in un ambiente sicuro e ne analizza il comportamento prima di consentirne l'accesso alla rete
- **Sistema di prevenzione delle intrusioni (IPS):** analizza il traffico di rete per rilevare e bloccare payload dannosi, exploit di vulnerabilità e tentativi di accesso non autorizzato
- **Filtro web e dei contenuti:** filtra e blocca l'accesso a siti web dannosi o inappropriati
- **Controllo e monitoraggio delle applicazioni:** identifica, classifica e controlla applicazioni specifiche per dare priorità al traffico importante e bloccare le app non autorizzate
- **Collaborative Detection & Response (CDR):** si collega ad altri dispositivi di rete per mettere in quarantena o bloccare automaticamente i dispositivi compromessi ai margini della rete
- **Supporto VPN robusto:** supporto sia per VPN IPSec per connessioni punto-punto, sia per VPN SSL per l'accesso remoto
- **Autoprotezione e reputazione IP:** protegge l'appliance firewall stessa disabilitando automaticamente le porte vulnerabili quando non in uso. Utilizza inoltre liste di blocco esterne e filtri basati sulla reputazione IP per fermare il traffico potenzialmente dannoso proveniente da fonti non autorizzate
- **Gestione cloud sicura Nebula:** è inclusa la licenza Nebula di livello base, che consente la configurazione e il monitoraggio da remoto di dispositivi e impostazioni

Clicca qui per maggiori dettagli.



Serie USG FLEX H: una nuova era nella cybersecurity.

Rendere visibile la protezione

È naturale voler vedere il valore di un investimento, soprattutto quando un'azienda non ha mai subito una violazione o un attacco.

La nostra dashboard cloud per l'analisi della sicurezza, SecuReporter, rende semplice capire quanto è efficace la protezione offerta dalla serie USG FLEX H.

SecuReporter mostra grafici e diagrammi chiari e facili da leggere, che permettono di avere una visione dell'attività di rete, compresa quella potenzialmente dannosa rilevata sulla rete. È un modo semplice e immediato per dimostrare il valore della protezione.

Con SecuReporter, le aziende possono vedere tutta l'attività di rete, compresi i file segnalati e analizzati nella cloud sandbox, così come i virus e i possibili tentativi di ransomware bloccati.

La piattaforma offre inoltre informazioni dettagliate sul comportamento degli utenti, ad esempio chi ha cliccato su un URL dannoso. Questo aiuta le aziende a capire dove intervenire sulla propria policy di sicurezza o sulla formazione del personale.



La nostra esperienza nella cybersecurity

Sebbene Zyxel Networks sia conosciuta soprattutto per le soluzioni di switching e gli access point WiFi, produciamo firewall dal 1999 e abbiamo una lunga esperienza nella cybersecurity.

Centinaia di migliaia di aziende in tutto il mondo si affidano alle nostre soluzioni per proteggere le proprie reti. Clienti finali e partner sanno di poter contare su Zyxel Networks per mantenere la gestione semplice senza rinunciare alla sicurezza.

Il nostro lavoro è riconosciuto anche dal settore. L'USG FLEX 50HP, il modello entry-level della gamma, ha vinto il premio Security Hardware of the Year ai PC Pro Excellence Awards 2025. Inoltre, abbiamo ottenuto lo status Champion nell'indagine sulla sicurezza Professional User Ratings (PUR) 2026 condotta dall'organizzazione di ricerca indipendente *techconsult*, sulla base del feedback di migliaia di esperti di sicurezza.

Test indipendenti condotti da The Tolly Group confermano le prestazioni e l'efficacia della serie USG FLEX H in termini di sicurezza, evidenziando l'elevata capacità di rilevamento dei malware e la protezione complessiva offerta dalla gamma.

Zyxel Networks è inoltre una CVE Numbering Authority (CNA) registrata, un riconoscimento che riflette il nostro impegno come fornitore di sicurezza responsabile, in grado di identificare e gestire costantemente le Common Vulnerabilities and Exposures (CVE) segnalate. I nostri prodotti supportano la conformità a standard quali PCI-DSS (finanza), HIPAA (sanità) e CIPA (istruzione) e sono pronti per supportare le esigenze legate a GDPR e NIS2.







VISUALIZZA I REPORT TOLLY COMPLETI

Zyxel USG FLEX H-Series vs. Ubiquiti Dream Machine: valutazione dell'efficacia anti-malware di firewall/gateway:

www.tolly.com/publications/225150

Zyxel USG FLEX 100H vs. SonicWall TZ270: valutazione dell'efficacia anti-malware e della licenza in abbonamento del firewall:

www.tolly.com/publications/225151

Perché siamo diversi e perché questo conta

La posizione di Zyxel Networks come fornitore riconosciuto di soluzioni di cybersecurity ci distingue nel mercato del networking.

Nessuna azienda moderna può fare a meno di una connettività sicura e affidabile. Per le PMI, siamo tra i pochi vendor in grado di combinare la semplicità, le prestazioni e il rapporto qualità-prezzo di cui le piccole imprese hanno bisogno.

Rendiamo la sicurezza semplice

Con la crescente complessità della cybersecurity, il nostro obiettivo è rimasto lo stesso: renderla il più semplice possibile per le PMI e per i rivenditori IT e gli installatori che le supportano. Eliminiamo le barriere rendendo la cybersecurity più facile da capire e da offrire: rapida da implementare e semplice da giustificare, gestire e supportare.

Per le PMI offriamo una soluzione tutto-in-uno che non scende a compromessi sulla sicurezza e che rimane aggiornata e protetta. Per i partner IT e gli installatori, significa poter rafforzare la fiducia dei clienti, sviluppare nuove opportunità di business e generare ricavi ricorrenti.



Copyright © 2026 Zyxel e/o le sue affiliate. Tutti i diritti riservati. Tutte le specifiche sono soggette a modifiche senza preavviso. Sebbene sia stata posta ogni cura per garantire l'accuratezza delle informazioni contenute in questa pubblicazione, né Zyxel né le sue consociate/affiliate si assumono responsabilità per eventuali errori o imprecisioni.

30/09/2026