

endian|OS

Il motore per una trasformazione digitale sicura

Tutti i prodotti Endian sono basati su EndianOS, un sistema operativo (OS) sicuro progettato per rispondere alle sfide della digitalizzazione e della convergenza degli ambienti IT e OT. Questo articolo spiega i vantaggi che gli utenti ne possono trarre.

Un sistema operativo (OS) gestisce le risorse di sistema di un computer e le rende disponibili ai programmi operativi. EndianOS è basato su Linux, un software open-source che offre l'opportunità di costruire soluzioni individuali su misura per esigenze specifiche. È il pilastro di tutte le soluzioni Endian, in grado di soddisfare le esigenze delle reti aziendali, come la connettività e la gestione di macchine, apparecchiature, reti, dispositivi e utenti.

La sicurezza è il principio guida e la base di tutte le fasi di sviluppo di EndianOS. Senza un solido sistema di sicurezza, qualsiasi progetto di digitalizzazione potrebbe diventare un serio rischio per l'azienda. Endian opera secondo il principio della "Security by Design", dando priorità alla sicurezza durante lo sviluppo e l'intero ciclo di vita del prodotto.

Grazie alla configurazione incentrata sulla sicurezza e all'integrazione di numerose misure di sicurezza, EndianOS è il cosiddetto "hardened Linux", caratterizzato da un'elevata resilienza contro le potenziali minacce.

EndianOS comprende diversi elementi che, se combinati, offrono le soluzioni necessarie per una trasformazione digitale sicura:

Soluzioni EndianOS

Struttura Zero-Trust

Con la trasformazione digitale che rende più incerti i confini aziendali, i concetti di sicurezza tradizionali diventano obsoleti. Una semplice differenziazione tra accesso interno ed esterno non è più sufficiente. Un'architettura Zero-Trust consente alle aziende di ridurre al minimo la superficie di attacco stabilendo criteri di accesso, autorizzazione e sicurezza a grana fine. Inoltre, un ambiente Zero-Trust garantisce una migliore conformità e requisiti di audit.



Visualizzazione della rete

Prima di implementare un modello Zero-Trust, è essenziale identificare e analizzare ogni dispositivo all'interno della rete. I metodi tradizionali sono costosi e impegnativi dal punto di vista delle risorse e spesso richiedono scansioni frequenti. La visualizzazione continua della rete, definita da Endian "Network Awareness", offre una rapida panoramica di tutti i dispositivi connessi, assicurando una protezione completa contro le minacce.



Micro-segmentazione

La micro-segmentazione è un componente dell'Architettura Zero-Trust, che consente di creare piccole zone di rete personalizzate. Con l'accesso limitato, il livello di sicurezza aumenta. Applicando criteri di sicurezza rigorosi per ogni zona, le aziende possono garantire che all'interno della rete vengano autorizzate solo le comunicazioni autorizzate, stabilendo connessioni sicure con autorizzazioni ridotte al minimo.



Componenti:

Firewall, NAT (Network Address Translation), VPN (Virtual Private Network)

Gestione delle minacce

La situazione delle minacce nel mondo digitale sta cambiando rapidamente. EndianOS contiene quindi diversi componenti che possono essere utilizzati per rilevare e impedire automaticamente gli attacchi prima che danneggino la rete aziendale.

Il rilevamento e la prevenzione delle intrusioni a pacchetti profondi vengono utilizzati per impostare e applicare i criteri di sicurezza. L'analisi dell'applicazione e dei protocolli garantisce inoltre che lo scambio di dati sia realmente autorizzato. In caso di dubbio, può essere bloccato, indipendentemente dall'indirizzo IP e dalla porta.



Componenti:

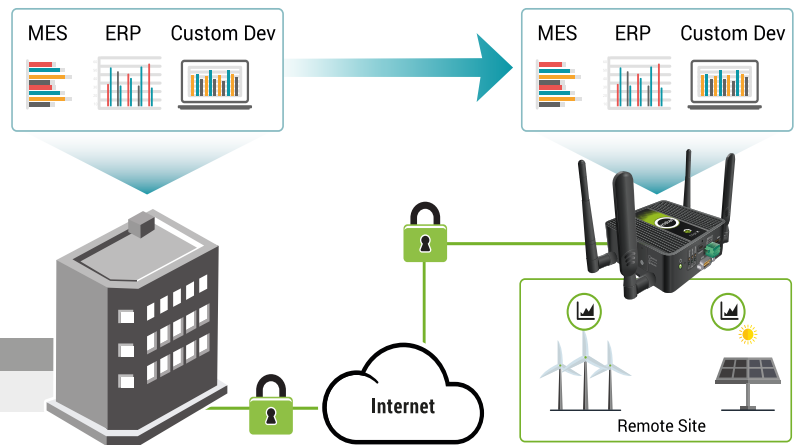
Firewall, IDS/IPS, Application, DNS Security

Edge Computing

L'edge computing si riferisce all'elaborazione decentralizzata di dati e calcoli direttamente alla fonte dei dati, invece di inoltrarli a un data center o a un cloud centralizzato. L'uso di Docker e delle tecnologie dei container consente il funzionamento delle applicazioni aziendali ai margini della rete, ampliando così l'ambito funzionale dell'edge computing.

Componenti:

Docker Engine



Componenti di EndianOS

Per implementare queste soluzioni, EndianOS include diversi componenti che garantiscono la connettività, la sicurezza e la gestione dell'infrastruttura:

Connettività

Soluzioni innovative come il Condition Monitoring o la "Predictive Maintenance" richiedono la raccolta e la valutazione costante dei dati. Con l'interconnessione di un numero sempre maggiore di macchine e sistemi, possono sorgere rapidamente problemi di larghezza di banda. Per ottimizzare la connettività, EndianOS offre diverse funzionalità:

Multi-WAN

Il componente Multi-WAN consente di utilizzare più connessioni Internet all'interno di una rete. Semplifica la distribuzione del traffico per migliorare la ridondanza e garantire la continuità delle operazioni aziendali.

Policy routing

L'uso del policy routing consente alle aziende di assegnare priorità e gestire il flusso del traffico di rete (e quindi la larghezza di banda) su più connessioni Internet. Ciò garantisce la disponibilità continua delle applicazioni aziendali fondamentali.

Gestione della larghezza di banda

Le aziende possono stabilire criteri per l'utilizzo della larghezza di banda disponibile. Le applicazioni specifiche per l'azienda ricevono la massima priorità, mentre le attività non importanti possono essere limitate o bloccate.

Alta affidabilità

L'High Availability riduce al minimo i tempi di inattività grazie al clustering di almeno due appliance, consentendo a una di esse di subentrare in caso di anomalia dell'altra per garantire la continuità aziendale.

La sicurezza

La sicurezza è alla base di una digitalizzazione di successo. La crescente interconnettività dei dispositivi, soprattutto negli ambienti industriali dove sempre più sistemi di tecnologia operativa (OT) sono connessi a Internet, amplia la superficie di attacco per i cybercriminali. Ciò richiede solide funzioni di sicurezza in EndianOS:

Firewall

Il firewall combina un'interfaccia utente intuitiva con funzioni innovative per garantire la sicurezza e l'efficienza della rete. Gli utenti possono creare, implementare e monitorare le regole individuali del firewall, come ad esempio l'inserimento nella lista nera delle applicazioni indesiderate o il blocco dell'accesso da paesi o regioni specifiche.

Rete privata virtuale (VPN) sicura

Tutte le comunicazioni sono protette da una rete privata virtuale (VPN), in modo che i dati siano crittografati e rimangano sempre protetti. La VPN di Endian può essere utilizzata per stabilire un accesso remoto sicuro a reti, macchine e impianti, nonché per creare una connessione sicura tra reti gestite.

Rilevamento delle intrusioni (IDS) e prevenzione delle intrusioni (IPS)

La scansione continua di tutti i pacchetti di dati, fino al livello delle applicazioni, identifica le linee di base del traffico di rete. Qualsiasi differenza rispetto a questa baseline viene rilevata dal sistema di rilevamento delle intrusioni (IDS). Se la differenza è dovuta a una minaccia, ad esempio un malware, il sistema di prevenzione delle intrusioni (IPS) la blocca.

Filtraggio DNS

Il filtraggio DNS utilizza il proxy DNS per bloccare i siti di phishing e altre minacce informatiche. Questo aggiunge un ulteriore livello di sicurezza. Di conseguenza, l'azienda può proteggere i propri dati e controllare l'accesso dei dipendenti alle proprie reti.

Management

Il numero crescente di dispositivi connessi comporta una certa complessità, aumentando il carico di lavoro amministrativo e favorendo errori che possono rapidamente trasformarsi in rischi per la sicurezza. Con EndianOS, la gestione della rete diventa più semplice, mentre gli approcci automatizzati garantiscono una maggiore sicurezza.

Visualizzazione della rete

La visualizzazione della rete assicura agli utenti una visione complessiva, indipendentemente dalla complessità delle loro reti. I dashboard rappresentano il traffico e le attività di rete in tempo reale. La funzione "Time Machine" fornisce una visione degli eventi di rete passati.

Aggiornamenti programmati

Soltanto strumenti di sicurezza aggiornati possono contrastare efficacemente le nuove minacce, difatti, EndianOS automatizza gli aggiornamenti per tutti i dispositivi connessi, garantendo che siano sempre aggiornati.

EndianOS - pronto per essere utilizzato da voi!

EndianOS offre alle organizzazioni la base ideale per una trasformazione digitale sicura, semplice e sostenibile. Il sistema operativo consente di scalare installazioni di rete più grandi e complesse, grazie al supporto di un numero (virtualmente) illimitato di zone di rete interne. Gli utenti possono aggiungere facilmente reti su richiesta e aumentare la sicurezza integrando funzioni di sicurezza di rete avanzate. Grazie al supporto dell'Edge Computing con Docker, gli utenti hanno anche la possibilità di eseguire applicazioni e servizi ai margini della rete.