IL PROBLEMA REALE

Ho già l’antivirus. Perché mi serve AI Defender?

Antivirus e cybersecurity non sono la stessa cosa.

L’antivirus è importante: protegge soprattutto il singolo computer da virus e software dannosi.

Molti attacchi informatici colpiscono aziende che l’antivirus lo hanno già.

Gli attacchi possono entrare anche da:

- una password rubata o riutilizzata;
- una falsa email aperta da un dipendente;
- un account Microsoft 365 compromesso;
- un aggiornamento mancante o una configurazione sbagliata;
- un accesso aziendale lasciato esposto.

L’antivirus protegge il PC.

AI Defender protegge il lavoro dell’azienda: email, password, accessi, dati, configurazioni e comportamenti.

CYBERSECURITY IN PAROLE SEMPLICI

La sicurezza dell’azienda nel mondo digitale.

Serve a impedire che qualcuno entri negli account, blocchi i computer, rubi dati, mandi email-truffa o interrompa l’attività.

I quattro problemi più comuni

01 EMAIL-TRUFFA

Un dipendente clicca un link falso e consegna password o dati.

02 COMPUTER BLOCCATI

Virus o ransomware fermano il lavoro e possono chiedere un riscatto.

03 ACCESSI RUBATI

Una password debole permette a terzi di entrare in posta e archivi.

04 DATI PERSI

File cancellati, cifrati o non recuperabili perché il backup non è adeguato.

Il punto non è eliminare ogni rischio.

Il punto è conoscere dove l’azienda è esposta, correggere prima le priorità e mantenere i controlli nel tempo.

IL METODO AI DEFENDER

Prima capiamo. Poi sistemiamo. Infine proteggiamo.

Un percorso progressivo, con decisioni comprensibili e azioni autorizzate.

01

CONTROLLA

Raccoglie evidenze su PC, software, accessi, Microsoft 365 e configurazioni.

02

SPIEGA

Traduce i problemi tecnici in rischi, priorità e decisioni comprensibili.

03

CORREGGE

Pianifica gli interventi autorizzati, partendo da ciò che può creare più danno.

04

SORVEGLIA

Mantiene aggiornati i controlli e supporta l’azienda quando accade qualcosa.

!

L’intelligenza artificiale accelera l’analisi. Le decisioni restano umane.

Le azioni importanti sono verificate e autorizzate da persone competenti.

COME INIZIARE

Un primo passo chiaro. Poi decidi tu.

Nessun contratto complesso al primo incontro.

01

ASSESSMENT GRATUITO

Audit endpoint Windows

- Fino a 20 PC
- Sola lettura
- Prime anomalie e configurazioni

02

€ 290 UNA TANTUM

Assessment organizzativo

- IT, cloud, backup e Microsoft 365
- Rischi e priorità
- Piano 30/60/90 giorni

03

SU PROGETTO

Add-on specialistici

- Dark web e dominio
- Server, firewall e IP
- Supporto specialistico

PROTEZIONE CONTINUA

Dopo la valutazione, il presidio può proseguire con livelli Essential, Pro, Elite o Enterprise, a partire da € 9 per PC al mese.

Il cliente vede subito cosa riceve, quanto costa e quale sarà il passo successivo.

Esempio: una PMI con 10 PC può iniziare dall’audit endpoint gratuito, aggiungere l’assessment organizzativo e decidere solo dopo se attivare la protezione continuativa.

PROTEZIONE CONTINUA

Quattro livelli. Una protezione che cresce con te.

Il piano Pro è la scelta consigliata per la maggior parte delle PMI.

CRITERIO	ESSENTIAL	PRO CONSIGLIATO	ELITE	ENTERPRISE
Prezzo	**€ 9 / PC / mese**	**€ 24 / PC / mese**	**€ 49 / PC / mese**	**A progetto**
Per chi	Piccole aziende o primo livello	**La maggior parte delle PMI**	Aziende che vogliono monitoraggio attivo	Multisede, oltre 20 dispositivi o necessità H24
Cosa cambia	Aggiornamenti, controlli e report trimestrale	**Protezione avanzata, MFA, controlli Microsoft 365, log e report**	Eventi anomali sorvegliati, presidio continuativo e report mensile	Controllo H24, minacce, tempi definiti e gestione completa
Scelta	**Minimo serio**	**RACCOMANDATO**	**Presidio strutturato**	**Soluzione su misura**

Condizioni essenziali

- Prezzi IVA esclusa; canoni annuali fatturati anticipatamente.
- Licenze Microsoft e servizi di backup non inclusi.
- Per Pro ed Elite sono richiesti requisiti tecnici adeguati, tra cui Windows 11 Pro e Microsoft 365 Business Premium.
- Gli interventi di sistemazione sono preventivati separatamente.

IL RISULTATO

Più controllo. Meno complessità.

Un percorso chiaro, con risultati visibili e decisioni comprensibili.

01 PRIMA VERIFICA

Audit endpoint gratuito e prime esposizioni evidenti.

02 REPORT E PIANO

Rischi, priorità e piano operativo 30/60/90 giorni.

03 PRESIDIO

Controlli periodici, protezione continuativa e supporto.

Cosa cambia per l’azienda

CONTINUITÀ

Ridurre il rischio che PC, posta o servizi si blocchino.

SEMPLICITÀ

Un referente che traduce la tecnica in decisioni chiare.

FIDUCIA

Proteggere clienti, dipendenti, fornitori e reputazione.

EVIDENZE

Documentare controlli, azioni e misure adottate nel tempo.

CLIENTI E FILIERA

Le evidenze aiutano a rispondere ai requisiti di clienti, partner e obblighi applicabili.

POLIZZE CYBER

Misure e procedure documentate possono supportare la gestione della polizza e di un eventuale sinistro.

Partiamo da un controllo tecnico preliminare gratuito.

Un primo passo semplice per capire le esposizioni principali e decidere cosa fare dopo.

Prezzi IVA esclusa. Licenze Microsoft, backup e lavori tecnici non inclusi salvo diversa offerta. Myma S.r.l. - Repubblica di San Marino