



AI DEFENDER · PRESIDIO CONTINUATIVO

Active Shield

La sicurezza delle informazioni,
seguita nel tempo.

PC, email, accessi, dati, persone e fornitori: più controllo, più continuità, più evidenze.

CHE COSA FA PER LA TUA ORGANIZZAZIONE

Un unico modello per valutare, correggere e presidiare.

Active Shield aiuta l'azienda a controllare nel tempo la propria sicurezza informatica e la sicurezza delle informazioni.

01 Capire

Starter Shield unisce audit endpoint e Assessment organizzativo AI Defender.

02 Correggere

Il Remediation Plan indica le azioni consigliate per chiudere i gap principali.

03 Presidiare

Con Active Shield si seguono dispositivi, aggiornamenti, vulnerabilità, persone, accessi e segnali di rischio.

04 Documentare

Report e sintesi aiutano responsabile IT, referenti e Direzione a capire priorità e risultati.

Non è un intervento una tantum.

È un percorso continuativo per ridurre progressivamente il rischio.



ACTIVE SHIELD · PERCHÉ SERVE

La sicurezza non è solo antivirus.

Molte aziende hanno già strumenti di protezione: antivirus, firewall, Microsoft 365, MFA, backup o fornitori IT. Il problema, spesso, è governarli nel tempo con priorità chiare, responsabilità definite e informazioni comprensibili.

DOVE NASCE IL RISCHIO

Computer non aggiornati

Software e sistemi non aggiornati possono diventare un punto debole.

Programmi vulnerabili

Un programma installato ma non controllato può esporre l'azienda.

Accessi da presidiare

Password, MFA, account amministrativi e utenti inattivi richiedono attenzione.

Persone esposte al phishing

Email ingannevoli e credenziali compromesse restano rischi concreti.

Fornitori da controllare

Quando intervengono più soggetti, serve sapere chi fa cosa.

Poche evidenze disponibili

Senza report e registri è difficile dimostrare attività e miglioramenti.

Active Shield aiuta a trasformare la sicurezza in un presidio continuativo.

Più visibilità, più controllo, più continuità.



ACTIVE SHIELD · COME SI PARTE

Prima valutiamo. Poi decidiamo.

Starter Shield chiarisce la situazione iniziale: serve a capire se l'azienda è già pronta per un presidio annuale o se deve prima completare alcune azioni minime.

01**Starter Shield**

Audit endpoint e Assessment organizzativo AI Defender.

**02****Remediation Plan**

Azioni consigliate e priorità.

**03****Active Shield**

Scelta del livello più adatto.

STARTER SHIELD COMPRENDE

Audit endpoint

Computer, software, aggiornamenti e vulnerabilità.

Assessment organizzativo

Strumenti, ruoli, fornitori, procedure e gestione quotidiana.

Analisi dei gap

Aree che aumentano il rischio o riducono l'efficacia del presidio.

Remediation Plan

Piano di miglioramento con priorità e azioni consigliate.

ADD-ON PER STARTER SHIELD

Approfondimenti opzionali per completare la fotografia iniziale**Dark Web / Exposure Report avanzato**

Verifica approfondita di credenziali aziendali, domini e dati esposti online.

TPRM Check

Valutazione preliminare dei fornitori IT, cloud e terze parti da cui dipende il lavoro.

EVA · External Vulnerability Assessment

Controllo delle vulnerabilità e dei servizi aziendali esposti su Internet.

Privacy & GDPR Check

Verifica di allineamento tra misure di sicurezza informatica e tutela dei dati personali.

Starter Shield aiuta l'azienda a scegliere, a propria discrezione, il livello Active Shield più adatto.



ACTIVE SHIELD · LIVELLI DI SERVIZIO

Scegli il livello più adatto.

Livelli diversi per esigenze e maturità differenti. L'obiettivo è costruire un presidio proporzionato, chiaro e sostenibile.

Essential

Controllo tecnico

- Controllo dei computer e inventario hardware e software.
- Aggiornamenti e verifica delle vulnerabilità.
- Reportistica essenziale.

Pro

Tecnologia e persone

- Base Essential sui PC inclusi.
- Protezione avanzata, controlli Microsoft 365 e MFA.
- **Human Shield Flex incluso:** simulazioni phishing e controllo delle credenziali esposte.
- Controlli e report più estesi.

Elite

Sorveglianza specialistica

- Servizi Pro con **Human Shield Full al posto di Flex:** formazione e distribuzione/tracciamento dei documenti e delle policy del cliente.
- **Vigilant Shield H24 incluso,** 7 giorni su 7.
- Gestione degli eventi previsti, report e azioni preventive.

Enterprise

Servizi su progetto

- Per più sedi o infrastrutture complesse.
- Integrazione con gli strumenti esistenti.
- Servizi e modalità operative definiti su misura.

Human Shield Flex non include formazione.

La scelta dipende dalle esigenze dell'azienda.

L'offerta specifica account, PC inclusi, attività, responsabilità e modalità operative.

L'H24 riguarda Vigilant Shield, non tutti gli interventi tecnici. Gli interventi straordinari o non inclusi sono concordati e quotati separatamente.



ACTIVE SHIELD · ADD-ON E REPORT

Cosa aggiungi. Cosa ricevi.

Gli add-on sono attivabili su richiesta quando l'azienda ha bisogno di maggiore documentazione, governo dei fornitori o verifica privacy/GDPR.

ADD-ON ACTIVE SHIELD

**Policy Pack /
Governance Pack**

Policy, procedure, registri, istruzioni cyber e documenti per utenti e fornitori.

TPRM Governance

Mappatura, classificazione e aggiornamento dei fornitori critici.

Privacy & GDPR Review

Collegamento tra sicurezza informatica, dati personali, accordi sul trattamento (DPA), conservazione e accessi.

CHE COSA RICEVI

Informazioni chiare per chi deve decidere.

Report periodici

Attività svolte, trend e stato del presidio.

Priorità

Aree da seguire e azioni consigliate.

Evidenze

Report, registri e attività documentate.

Coordinamento

Ruoli più chiari tra AI Defender, IT e fornitori.

Active Shield rende il rischio più leggibile e aiuta a decidere meglio.



ACTIVE SHIELD · ATTIVAZIONE E GOVERNO

Un servizio definito insieme.

COME FUNZIONA IL PRESIDIO NEL TEMPO

- 01 Definiamo perimetro e ruoli.** Individuiamo computer, utenti, strumenti attivi, fornitori e referenti interni, chiarendo subito chi fa cosa tra azienda, IT incaricata e AI Defender.
- 02 Allineiamo la baseline iniziale.** Usiamo le evidenze di Starter Shield e del Remediation Plan per chiudere i gap prioritari e attivare il livello Active Shield scelto (Essential, Pro, Elite o Enterprise).
- 03 Presidiamo controlli e scadenze.** Seguiamo nel tempo aggiornamenti, vulnerabilità, accessi, esposizioni e prontezza delle persone, secondo le routine concordate.
- 04 Coordiniamo priorità ed eventi.** Quando emergono anomalie, punti aperti o incidenti significativi, aiutiamo IT e Direzione a classificare il problema, decidere le azioni e mantenere il controllo.
- 05 Documentiamo risultati e miglioramenti.** Consegniamo report periodici, registri ed evidenze verificabili per misurare i progressi, aggiornare il rischio residuo e pianificare i passi successivi.

Che cosa viene precisato nell'offerta

- Livello Active Shield attivato.
- Numero di computer e utenti inclusi.
- Attività comprese ed escluse.
- Eventuali add-on.
- Frequenza dei report.
- Ruoli e responsabilità.

Cosa non è Active Shield

- Non è un penetration test.
- Non garantisce l'assenza di incidenti.
- Non sostituisce l'IT interno.
- Non sostituisce il fornitore tecnico.
- Non è un servizio legale o privacy completo.
- Non è una certificazione.

PICCOLO GLOSSARIO

Endpoint: Computer fisso o portatile utilizzato per lavorare.

Vulnerabilità: Punto debole di un software, sistema o configurazione.

Remediation Plan: Piano di azioni per correggere i gap rilevati.

Patch: Aggiornamento che corregge errori o problemi di sicurezza.

MFA: Controllo aggiuntivo oltre alla password.

TPRM: Gestione del rischio legato a fornitori e terze parti.

Vuoi capire da dove partire?

Inizia con Starter Shield (audit endpoint, Assessment organizzativo AI Defender e Remediation Plan) oppure consulta online caratteristiche e prezzi trasparenti dei livelli Active Shield.

MYMA S.r.l. · AI Defender

Via del Serrone 62, 47890 Murata (RSM)

info@myma.sm

www.myma.sm/active-shield