SYNSPHERE

WHITE PAPER · GIUGNO 2026

Mettere in sicurezza Microsoft 365: framework operativo per le PMI

Identità, posta, endpoint, dati e monitoraggio: le misure essenziali in ordine di priorità, dal Secure Score al piano di risposta.

synsphere.it

In sintesi

La sicurezza di Microsoft 365 non si compra: si configura. Questo white paper propone un framework operativo in cinque livelli — identità, posta elettronica, endpoint, dati e monitoraggio — pensato per le PMI italiane che vogliono proteggere il proprio tenant senza budget enterprise. Per ogni livello indichiamo le misure essenziali in ordine di priorità, dagli strumenti già inclusi nelle licenze Business fino al piano di risposta agli incidenti. Chiudono il documento una roadmap per livelli di maturità e una checklist operativa pronta all'uso.

Mettere in sicurezza Microsoft 365: framework operativo per le PMI — Prima edizione: giugno 2026.

Indice

1. Il panorama delle minacce per le PMI italiane

«Siamo troppo piccoli per interessare a un criminale informatico» è probabilmente la frase più pericolosa che si possa pronunciare in una PMI. Gli attacchi moderni non scelgono il bersaglio sfogliando le classifiche di fatturato: sono campagne automatizzate che colpiscono migliaia di organizzazioni contemporaneamente e si fermano dove trovano una porta aperta. Una PMI con MFA assente, posta non protetta e backup improvvisati è una porta aperta, indipendentemente dalle sue dimensioni. Anzi: proprio perché gli attaccanti sanno che le difese delle piccole imprese sono mediamente più deboli, le PMI sono diventate un bersaglio privilegiato, non un bersaglio di ripiego.

Il secondo equivoco riguarda il cloud: migrare su Microsoft 365 non significa essere automaticamente al sicuro. Microsoft protegge l'infrastruttura — i datacenter, la piattaforma, la disponibilità del servizio — ma la configurazione del tenant, le identità degli utenti e i dati restano responsabilità del cliente. È il cosiddetto **modello di responsabilità condivisa**, e la maggior parte degli incidenti che si osservano sul campo nasce proprio dal lato cliente: configurazioni di default mai riviste, permessi eccessivi, utenti non formati.

Le quattro minacce che contano davvero

- **Phishing e furto di credenziali**: email che imitano Microsoft, corrieri, banche o fornitori per sottrarre username e password. È il vettore d'ingresso più comune in assoluto, perché nel cloud la credenziale è la chiave di tutto.
- **Business Email Compromise (BEC)**: l'attaccante compromette o imita la casella di un dirigente o di un fornitore e dirotta pagamenti veri verso coordinate fraudolente. Non serve malware: bastano ingegneria sociale e pazienza.
- **Ransomware**: cifratura dei dati aziendali con richiesta di riscatto, sempre più spesso accompagnata dall'esfiltrazione preventiva dei dati e dalla minaccia di pubblicarli (la cosiddetta double extortion).
- **Account takeover**: il controllo completo di un account Microsoft 365 legittimo, usato poi per leggere la posta, creare regole di inoltro nascoste e muoversi lateralmente verso colleghi, clienti e fornitori.

Minaccia	Come inizia di solito	Cosa cerca l'attaccante
Phishing	Email con link a false pagine di login	Credenziali Microsoft 365
BEC	Account compromesso o dominio simile al vero	Dirottare bonifici e pagamenti
Ransomware	Allegato malevolo, vulnerabilità non corretta	Riscatto ed esfiltrazione dati
Account takeover	Credenziali rubate o sessione intercettata	Persistenza nel tenant, frodi

Il filo conduttore è evidente: quasi tutti questi attacchi iniziano da un'identità. Una credenziale rubata via phishing apre la strada al BEC, all'account takeover e spesso anche al ransomware. Ecco perché il framework che proponiamo nelle prossime sezioni non parte dal firewall né dall'antivirus, ma dall'identità.

2. Il modello a livelli: perché si parte dall'identità

Nel mondo on-premises il perimetro era la rete: dentro fidato, fuori ostile. Con Microsoft 365 quel perimetro non esiste più. Si lavora da casa, dal cliente, dal telefono; i dati stanno in Exchange Online, SharePoint e OneDrive; le applicazioni si raggiungono da qualunque rete. L'unico elemento che accompagna ogni accesso, ovunque avvenga, è l'identità dell'utente gestita da Microsoft Entra ID. Per questo si parla di **identity-first security**: l'identità è il nuovo perimetro, e da lì si comincia.

Il framework che usiamo in SynSphere sui +150 tenant Microsoft 365 che gestiamo è organizzato in cinque livelli progressivi, ordinati per rapporto tra beneficio e sforzo. Non è una classifica accademica: è l'ordine in cui conviene davvero investire tempo e attenzione, perché ogni livello riduce drasticamente l'efficacia degli attacchi descritti nella sezione precedente.

1. **Identità**: MFA, Conditional Access, ruoli amministrativi minimi. Blocca la stragrande maggioranza degli attacchi basati su credenziali rubate.
2. **Posta elettronica**: autenticazione del dominio (SPF, DKIM, DMARC) e filtri avanzati su link e allegati. Riduce phishing e BEC.
3. **Endpoint**: dispositivi gestiti, cifrati, aggiornati e dotati di EDR. Contiene malware e ransomware.
4. **Dati**: classificazione, DLP, conservazione e backup. Limita il danno quando qualcosa sfugge ai livelli precedenti.
5. **Monitoraggio e risposta**: Secure Score, audit log, alert e piano di risposta agli incidenti. Trasforma la sicurezza da progetto a processo.

Due avvertenze prima di entrare nel merito. La prima: i livelli non sono alternativi ma cumulativi — un tenant con MFA perfetta ma posta non protetta resta vulnerabile al BEC, e un parco endpoint blindato non salva da una credenziale amministrativa rubata. La seconda: quasi tutto ciò che descriviamo nelle sezioni che seguono è già incluso nelle licenze Microsoft 365 Business Premium o disponibile come componente aggiuntivo. Il problema delle PMI raramente è il budget per gli strumenti: molto più spesso è il fatto che gli strumenti già pagati non sono mai stati configurati.

Un'ultima nota di metodo, che vale per ogni sezione di questo documento: ogni misura andrebbe prima testata su un gruppo pilota, poi comunicata agli utenti con istruzioni semplici, poi estesa a tutti. La sicurezza imposta dall'oggi al domani genera ticket, frustrazione e — peggio ancora — workaround creativi che aprono falle nuove. Il fattore umano non si configura da un portale: si accompagna.

3. Identità: MFA, Conditional Access e privilegi minimi

Se questo white paper dovesse ridursi a una sola misura, sarebbe questa: **autenticazione a più fattori (MFA) per tutti gli utenti, senza eccezioni**. La quasi totalità degli attacchi basati su credenziali rubate fallisce contro un secondo fattore ben configurato. Microsoft stessa ha reso obbligatoria la MFA per l'accesso ai portali di amministrazione: il segnale è chiaro, la password da sola non è più una protezione accettabile.

MFA per tutti, con metodi resistenti al phishing

Non tutti i metodi MFA si equivalgono. Le passkey (FIDO2) e Windows Hello for Business sono resistenti al phishing per costruzione: non c'è un codice da digitare che una pagina falsa possa intercettare. L'app Microsoft Authenticator con number matching è il compromesso pratico per la maggior parte delle PMI. SMS e telefonate restano meglio di niente, ma vanno considerati un ripiego temporaneo: i kit di phishing moderni sanno intercettare anche i codici usa e getta, con tecniche adversary-in-the-middle che rubano direttamente la sessione autenticata.

Conditional Access: il cervello delle regole di accesso

I security defaults di Microsoft Entra ID sono il punto di partenza gratuito: impongono la MFA e bloccano l'autenticazione legacy. Ma per una PMI che vuole regole su misura serve il **Conditional Access**, incluso in Entra ID P1 e quindi in Microsoft 365 Business Premium. Le policy fondamentali da cui partire:

- Richiedere MFA a tutti gli utenti per qualsiasi applicazione cloud.
- Bloccare i protocolli di autenticazione legacy, che aggirano la MFA per costruzione.
- Bloccare o sottoporre a verifica aggiuntiva gli accessi da Paesi in cui l'azienda non opera.
- Richiedere un dispositivo conforme (vedi sezione 5) per accedere ai dati aziendali.
- Imporre criteri più severi agli account amministrativi: solo da dispositivi gestiti, con sessioni brevi.

Ogni policy va creata prima in modalità report-only, osservando per qualche giorno chi verrebbe bloccato, e solo dopo attivata. È la differenza fra un rollout ordinato e un lunedì mattina di telefonate al centralino.

Ruoli amministrativi: il minimo indispensabile

Il ruolo di amministratore globale dovrebbe essere un'eccezione, non la norma: Microsoft raccomanda di limitarne il numero a poche unità anche nei tenant grandi e di usare ruoli specifici — Exchange Administrator, User Administrator, Helpdesk Administrator — per i compiti quotidiani. Gli account amministrativi devono inoltre essere separati dagli account di lavoro di tutti i giorni: l'amministratore non naviga, non legge la posta e non apre allegati con l'account privilegiato. Chi dispone di Entra ID P2 può fare un passo ulteriore con Privileged Identity Management, che assegna i privilegi solo quando servono e per il tempo strettamente necessario.

Account break-glass: la porta di emergenza

Prima di stringere le viti, create due account di emergenza (break-glass): account cloud-only con ruolo di amministratore globale, esclusi dalle policy di Conditional Access, protetti da credenziali molto robuste — idealmente una passkey FIDO2, in alternativa una password lunghissima generata casualmente e custodita in cassaforte. Servono a rientrare nel tenant se una policy mal configurata o un disservizio del provider MFA chiude fuori tutti gli amministratori. Ogni loro utilizzo deve generare un alert immediato: se un break-glass si autentica, qualcuno deve accorgersene entro pochi minuti.

Password: lunghe, uniche, senza scadenza forzata

Può sembrare controintuitivo, ma sia Microsoft sia le principali linee guida internazionali sconsigliano ormai la scadenza periodica forzata delle password: spinge gli utenti verso varianti prevedibili che un attaccante indovina al primo tentativo. Meglio password lunghe e uniche, mai riutilizzate altrove, idealmente generate da un password manager, abbinate alla protezione password di Entra ID che blocca i termini più comuni e le varianti del nome aziendale. Con una MFA solida e il monitoraggio attivo, la scadenza forzata aggiunge attrito senza aggiungere sicurezza.

> **Il consiglio SynSphere**
> Prima di attivare la MFA per tutti, estraete l'elenco degli utenti che ne sono ancora privi e dei protocolli legacy ancora in uso: quasi ogni tenant ha una stampante multifunzione, un gestionale o una casella di servizio che invia posta con autenticazione di base. Censiteli, migrateli o create eccezioni controllate e documentate, e il rollout fila liscio. È il primo passo che facciamo in ogni assessment: nei tenant mai irrobustiti prima, le sorprese non mancano mai.

4. Posta elettronica: autenticare il dominio, filtrare le minacce

La posta elettronica resta il canale d'attacco preferito, per una ragione semplice: funziona. La difesa si gioca su due fronti complementari: **autenticare il proprio dominio**, perché nessuno possa spedire email spacciandosi per la vostra azienda, e **filtrare la posta in arrivo**, perché phishing e malware non raggiungano gli utenti.

SPF, DKIM e DMARC: la carta d'identità del vostro dominio

I tre record DNS dell'autenticazione email lavorano insieme. SPF dichiara quali server sono autorizzati a inviare posta per il dominio; DKIM firma crittograficamente ogni messaggio in uscita; DMARC dice ai server riceventi cosa fare dei messaggi che falliscono i controlli e consente di ricevere report aggregati su chi sta usando il vostro dominio. Configurarli correttamente protegge clienti e fornitori dallo spoofing del vostro marchio e migliora la deliverability dei messaggi legittimi.

Record	A cosa serve	Attenzione a
SPF	Elenca i server autorizzati a inviare per il dominio	Includere tutti i servizi che spediscono (CRM, newsletter), limite dei lookup DNS
DKIM	Firma crittografica dei messaggi in uscita	Va abilitato per ogni dominio personalizzato, non solo per quello principale
DMARC	Policy sui messaggi che falliscono i controlli, report	Partire da p=none, analizzare i report, poi salire a quarantine e reject

L'errore tipico è pubblicare DMARC con policy p=none e fermarsi lì: i report arrivano, nessuno li legge, la policy non viene mai inasprita e la protezione effettiva resta nulla. Il percorso corretto è graduale: p=none per qualche settimana per censire tutte le sorgenti legittime (gestionale, piattaforma newsletter, sito web), poi p=quarantine, infine p=reject. Solo con reject il dominio è

davvero protetto dallo spoofing.

Anti-phishing, Safe Links e Safe Attachments

Microsoft Defender for Office 365 Piano 1, incluso in Business Premium, aggiunge tre protezioni che la posta standard non ha. Le policy anti-phishing con protezione dall'impersonificazione riconoscono i messaggi che imitano i vostri dirigenti o i domini dei vostri partner: è il cuore della difesa contro il BEC. **Safe Links** riscrive gli URL e li verifica al momento del clic, non solo alla consegna: un link che diventa malevolo due ore dopo l'invio viene comunque bloccato. **Safe Attachments** fa detonare gli allegati sospetti in una sandbox prima di consegnarli alla casella.

Il modo più rapido per attivare tutto con valori sensati sono le preset security policies: il profilo Standard va bene per la maggior parte delle PMI, lo Strict per chi tratta dati particolarmente sensibili. Aggiungete poi la protezione dall'impersonificazione indicando i nomi dei dirigenti e i domini dei partner critici, che i preset non possono conoscere da soli.

Regole di inoltro esterno: il segnale da non ignorare

Quando un attaccante compromette una casella, una delle prime mosse è creare una regola di inoltro automatico verso un indirizzo esterno: così continua a leggere la posta anche dopo che la password è stata cambiata. Exchange Online blocca di default l'inoltro automatico verso l'esterno tramite la policy di posta indesiderata in uscita: verificate che questa impostazione non sia stata allentata nel tempo. E auditate periodicamente le regole delle caselle — incluse quelle lato client — perché una regola che sposta messaggi in cartelle nascoste o li elimina è uno degli indicatori più affidabili di compromissione in corso.

> **Il consiglio SynSphere**
>
> Trattate i report DMARC come un impegno ricorrente, non come un progetto una tantum: uno strumento che li aggreghi e un controllo mensile di dieci minuti bastano per accorgersi sia delle sorgenti legittime dimenticate sia dei tentativi di spoofing. E quando attivate un nuovo servizio che invia email a nome vostro, l'aggiornamento di SPF e DKIM deve far parte della procedura di attivazione, non essere un ricordo a posteriori.

5. Endpoint: dispositivi gestiti, cifrati e aggiornati

Un'identità protetta che si autentica da un PC compromesso è una protezione dimezzata: il malware che vive sul dispositivo vede tutto ciò che vede l'utente, sessione autenticata inclusa. Per questo il terzo livello del framework riguarda gli endpoint — PC, Mac, smartphone e tablet — e si appoggia a due strumenti inclusi in Microsoft 365 Business Premium: **Intune** per la gestione e **Defender for Business** per la protezione.

Microsoft Intune: la regia dei dispositivi

Intune permette di registrare i dispositivi aziendali, applicare configurazioni coerenti (cifratura, firewall, requisiti di blocco schermo) e definire policy di conformità: un dispositivo che non rispetta i requisiti — protezione disattivata, sistema operativo obsoleto, dispositivo manomesso — viene marcato come non conforme. La vera forza arriva combinando Intune con il Conditional Access della sezione 3: si può imporre che ai dati aziendali accedano solo dispositivi conformi, chiudendo la porta a PC sconosciuti e macchine personali non gestite.

Defender for Business: oltre l'antivirus

Defender for Business porta nelle PMI capacità che fino a pochi anni fa erano appannaggio delle grandi aziende: rilevamento e risposta sugli endpoint (EDR), che osserva i comportamenti e non solo le firme; regole di riduzione della superficie di attacco (ASR), che bloccano per esempio i contenuti eseguibili creati dalle app Office o i processi figli anomali delle applicazioni di produttività; gestione delle vulnerabilità, che segnala software obsoleti e configurazioni deboli; e la possibilità di isolare un dispositivo dalla rete con un clic dalla console — fondamentale, come vedremo, nella risposta a un ransomware.

Patching: la manutenzione che previene

Una parte consistente delle compromissioni sfrutta vulnerabilità per cui la correzione esisteva già da settimane o mesi. Con gli update ring di Intune si governa la distribuzione degli aggiornamenti Windows per gruppi: un anello pilota che riceve subito gli update, il resto dell'azienda a seguire con qualche giorno di scarto per intercettare eventuali problemi. Non dimenticate ciò che sta fuori da Windows Update: browser, software gestionali, driver e firmware. E i riavvii: un aggiornamento installato ma in attesa di riavvio da tre settimane non protegge nessuno.

BitLocker: il furto del portatile non diventa data breach

La cifratura del disco con BitLocker, distribuita centralmente via Intune con le chiavi di ripristino custodite in Entra ID, trasforma il furto o lo smarrimento di un portatile da potenziale violazione di dati personali a semplice perdita di hardware. È una misura senza costi aggiuntivi di licenza e con impatto quasi nullo sugli utenti: non c'è motivo per non attivarla su tutta la flotta. E in caso di audit o di incidente, poter dimostrare che i dati sul dispositivo perso erano cifrati cambia radicalmente le valutazioni sulla necessità di notifica.

BYOD: il telefono personale con la posta aziendale

Nelle PMI il dispositivo personale con accesso alla posta è la norma, non l'eccezione. La risposta non è vietare (non funziona) né gestire integralmente il telefono del dipendente (sproporzionato e invasivo): le **app protection policy** di Intune proteggono i soli dati aziendali dentro le app Microsoft — PIN per aprirle, blocco del copia-incolla verso le app personali, cancellazione selettiva dei dati aziendali quando il collaboratore lascia l'azienda — lasciando intatta la sfera privata. È l'equilibrio giusto fra sicurezza dei dati e rispetto delle persone, ed è anche molto più facile da far accettare di una gestione completa del dispositivo.

6. Dati: classificare, prevenire le fughe e fare backup

I primi tre livelli proteggono le vie d'accesso; il quarto protegge ciò che conta davvero, cioè i dati. Qui entrano in gioco gli strumenti Microsoft Purview inclusi in Business Premium — etichette di riservatezza, prevenzione della perdita di dati, conservazione — e una componente che la piattaforma da sola non risolve: il backup.

Sensitivity labels: la classificazione che viaggia col file

Le etichette di riservatezza permettono di classificare documenti ed email (per esempio: Pubblico, Interno, Riservato, Strettamente riservato) e di associare alla classificazione protezioni concrete: cifratura, restrizioni all'inoltro, filigrane. La protezione viaggia con il file: un documento Riservato resta cifrato anche se finisce su una chiavetta USB o in un allegato spedito alla persona sbagliata. Il consiglio pratico è partire con uno schema semplice, tre o quattro etichette al massimo, con nomi che chiunque capisce al volo: gli schemi di classificazione barocchi falliscono sempre, perché nessuno li usa.

DLP: fermare l'errore prima che esca

Le policy di prevenzione della perdita di dati (DLP) intercettano i dati sensibili in movimento: un'email con decine di codici fiscali diretta a un dominio esterno, un file con coordinate bancarie condiviso pubblicamente da OneDrive. Purview include tipi di informazione sensibile già pronti per il contesto italiano — codice fiscale, IBAN, numeri di carta di pagamento — su cui costruire le prime policy senza partire da zero. Iniziate in modalità di solo monitoraggio: per qualche settimana la policy registra senza bloccare, voi calibrate le soglie sulle abitudini reali dell'azienda, poi attivate prima gli avvisi educativi all'utente e solo dopo i blocchi veri e propri.

Retention: conservare quanto serve, non per sempre

Le policy di conservazione garantiscono che email e documenti restino disponibili per il periodo richiesto da esigenze legali o fiscali anche se un utente li cancella, e che vengano eliminati quando il periodo scade — un principio che il GDPR chiama limitazione della conservazione. Attenzione però all'equivoco più diffuso in assoluto: **la retention non è un backup**. Protegge dalla cancellazione, non dal disastro, e non offre un ripristino massivo, rapido e puntuale nel tempo.

Perché serve un backup vero

Il modello di responsabilità condivisa è esplicito: Microsoft garantisce la disponibilità del servizio, il cliente resta responsabile dei propri dati. Cestini e versioning aiutano negli incidenti piccoli, ma hanno finestre temporali limitate e non sono pensati per il ripristino su larga scala: un ransomware che cifra i file sincronizzati con OneDrive, un offboarding gestito male, una cancellazione dolosa scoperta dopo mesi richiedono un backup separato, con copie immutabili che nemmeno un amministratore compromesso possa alterare e con punti di ripristino granulari. Le opzioni oggi non mancano, dalle soluzioni di terze parti consolidate all'offerta di backup nativa di Microsoft: ciò che non può mancare è il test di ripristino periodico, perché un backup mai testato è una speranza, non una misura di sicurezza.

> **Il consiglio SynSphere**
>
> Nei nostri assessment la domanda «se cancellassi questo file adesso, fra sei mesi lo recupereresti?» mette in difficoltà più aziende di qualsiasi discussione sulle policy. Definite per iscritto cosa viene salvato, con quale frequenza, con quale periodo di conservazione e chi è autorizzato al ripristino — e fate un test di restore almeno due volte l'anno, verbalizzandone l'esito. In un audit, quel verbale vale più di dieci slide di presentazione.

7. Monitoraggio continuo: Secure Score, audit log e alert

Tutto ciò che abbiamo configurato finora si degrada nel tempo: arrivano utenti nuovi, qualcuno crea eccezioni «temporanee» che diventano permanenti, Microsoft introduce funzionalità che andrebbero valutate. Il quinto livello trasforma la sicurezza da progetto con una data di fine a processo continuo, con tre strumenti già inclusi nel tenant.

Microsoft Secure Score: la bussola

Il Secure Score, nel portale Microsoft Defender, misura la postura di sicurezza del tenant con un punteggio percentuale e — soprattutto — propone un elenco prioritizzato di azioni di miglioramento, ciascuna con il proprio impatto stimato. Va letto con intelligenza: l'obiettivo non è il 100%, che può richiedere licenze o vincoli sproporzionati per una PMI, ma un miglioramento costante e consapevole. Una revisione mensile di trenta minuti — cosa è cambiato, quali azioni nuove sono apparse, cosa implementiamo questo mese — vale più di un progetto annuale calato dall'alto. E le azioni vanno valutate una per una: alcune sono quick win da fare subito, altre vanno pianificate con calma, altre ancora si possono motivatamente accettare come rischio residuo, documentando la scelta.

Unified audit log: la scatola nera del tenant

Il registro di controllo unificato registra le attività di utenti e amministratori in tutti i servizi: accessi, condivisioni di file, creazione di regole di posta, modifiche ai permessi, azioni amministrative. Nei tenant recenti è attivo di default, con una conservazione di circa sei mesi nella versione standard: verificate che lo sia davvero e, se i vostri obblighi di conformità richiedono di più, esportate i log verso una conservazione esterna di lungo periodo. Quando si indaga un sospetto di compromissione, l'audit log è la prima fonte di verità: chi ha fatto cosa, da dove, quando e su quali dati.

Alert: il tenant che vi avvisa da solo

Il portale Defender include policy di avviso predefinite per gli eventi più significativi: creazione di regole di inoltro sospette, rilevamenti malware, escalation di privilegi, accessi ad alto rischio. Il punto debole, nelle PMI, non è la generazione degli alert ma la loro destinazione: se finiscono in una casella che nessuno legge, è come se non esistessero. Indirizzateli verso una casella presidiata o un canale Teams dedicato, definite chi li guarda e con quale priorità, e stabilite un rituale settimanale di revisione con un responsabile chiaro.

Quando il volume di segnali cresce o servono correlazioni più sofisticate fra fonti diverse, il passo successivo è un SIEM cloud come Microsoft Sentinel. Ma per la maggior parte delle PMI gli strumenti inclusi nelle licenze, usati con disciplina, coprono già l'essenziale: il monitoraggio è soprattutto una questione di continuità organizzativa, ed è il livello in cui un partner esterno con un servizio gestito aggiunge più valore, perché presidiare alert e log richiede una costanza che un reparto IT di una o due persone fatica a garantire da solo.

8. Prepararsi al peggio: il piano di risposta agli incidenti

Anche il tenant meglio configurato può subire un incidente: una credenziale rubata con tecniche nuove, un fornitore compromesso, un errore umano. La differenza fra un inconveniente gestito e una crisi aziendale la fanno quasi sempre la velocità e l'ordine della risposta — e velocità e ordine, sotto stress, esistono solo se sono stati scritti prima, a mente fredda.

Un piano di risposta agli incidenti per una PMI non deve essere un tomo da cento pagine. Deve definire poche cose, ma bene: chi decide (e chi lo sostituisce se è irreperibile), chi esegue le azioni tecniche, chi comunica con dipendenti, clienti e autorità; come si classifica la gravità di un incidente; i playbook per gli scenari più probabili — account compromesso, ransomware, BEC, perdita di dati; e gli obblighi normativi, dalle 72 ore per la notifica al Garante in caso di violazione di dati personali ai termini ancora più stretti previsti dalla direttiva NIS2 per i soggetti che vi rientrano.

Account compromesso: la prima ora

1. Revocare tutte le sessioni attive dell'account dal portale di amministrazione: il solo cambio password non basta, le sessioni rubate sopravvivono.
2. Reimpostare la password e verificare i metodi MFA registrati: l'attaccante potrebbe aver aggiunto un proprio dispositivo come secondo fattore.
3. Controllare ed eliminare le regole di inoltro e le regole di posta create di recente, incluse quelle nascoste lato client.
4. Esaminare l'audit log: da dove si è autenticato l'attaccante, cosa ha letto, cosa ha inviato e a chi.
5. Verificare se dall'account compromesso sono partiti messaggi di phishing verso colleghi, clienti o fornitori, e avvisare i destinatari.
6. Documentare tutto con orari e screenshot: servirà per le notifiche alle autorità, per l'assicurazione e per le lezioni apprese.

Per il ransomware il playbook cambia: isolare immediatamente i dispositivi colpiti (Defender for Business lo consente direttamente dalla console), non spegnere le macchine se non indicato dagli specialisti per non perdere evidenze utili, attivare il ripristino dal backup e valutare con il supporto legale gli obblighi di notifica. La decisione sul riscatto non si improvvisa a sistemi fermi: la posizione di principio — non pagare — va discussa e messa a verbale prima, insieme al ruolo dell'eventuale polizza assicurativa.

Infine, il piano va provato: un'esercitazione tabletop di mezza giornata all'anno — si simula a voce un incidente e si percorre il piano passo per passo — fa emergere i buchi reali (numeri di telefono non aggiornati, fornitori senza reperibilità, backup che nessuno sa ripristinare) molto meglio di qualsiasi revisione documentale. È lo stesso approccio che applichiamo come SynSphere nei percorsi di adeguamento dei nostri clienti, ed è uno dei motivi per cui i clienti che accompagniamo hanno superato il 100% degli audit di compliance affrontati.

> **Il consiglio SynSphere**
> Scrivete il piano quando va tutto bene e stampatene una copia: se il ransomware cifra anche il file server o blocca l'accesso a SharePoint, il piano salvato solo lì dentro non vi servirà a nulla. Stessa logica per i contatti di emergenza: la lista con i telefoni di direzione, IT, fornitori critici e assicurazione deve esistere anche fuori dai sistemi aziendali.

9. Roadmap per livelli di maturità

Nessuna PMI può — né deve — implementare tutto questo in un mese. La roadmap che segue distribuisce le misure su tre livelli di maturità: il livello base si raggiunge in poche settimane e abbatte già la maggior parte del rischio; l'intermedio richiede tipicamente un trimestre di lavoro ordinato; l'avanzato è un'evoluzione continua, da affrontare quando i primi due livelli sono consolidati e presidiati.

Area	Base	Intermedio	Avanzato
Identità	MFA per tutti, blocco legacy auth, break-glass	Conditional Access su misura, ruoli minimi, filtri geografici	PIM, passkey FIDO2, accesso solo da dispositivi conformi
Posta	SPF e DKIM attivi, DMARC p=none, preset Standard	DMARC a quarantine o reject, anti-impersonificazione	Preset Strict, simulazioni di phishing ricorrenti
Endpoint	Defender attivo, BitLocker, aggiornamenti automatici	Enrollment Intune, policy di conformità, regole ASR	EDR presidiato, vulnerability management, BYOD con app protection
Dati	Cestini e versioning verificati, backup attivato	Etichette di riservatezza, DLP in solo monitoraggio	DLP in blocco, retention per categoria, test di restore
Monitoraggio	Secure Score letto, alert verso casella presidiata	Revisione mensile Secure Score, uso dell'audit log	Log esportati, SIEM (Sentinel), revisioni trimestrali
Risposta	Contatti di emergenza scritti e stampati	Piano di risposta formale con playbook per scenario	Tabletop annuale, raccordo con assicurazione e legale

Come usare la roadmap: scattate una fotografia onesta del livello attuale per ciascuna area — lo strumento naturale è il Secure Score, integrato da un assessment puntuale — e portate tutte le aree al livello base prima di spingere una singola area verso l'avanzato. Un tenant con identità avanzata e backup inesistente è più fragile di un tenant tutto a livello base. Formalizzate poi i passaggi di livello: una riga in un verbale di riunione basta, ma trasforma la sicurezza da attività episodica a percorso tracciabile, anche agli occhi di clienti, assicurazioni e auditor.

Una nota sulle licenze, senza entrare nei listini: quasi tutto ciò che serve per i livelli base e intermedio è incluso in Microsoft 365 Business Premium — Entra ID P1, Intune, Defender for Business, Defender for Office 365 Piano 1 e le funzioni Purview di base. Se la vostra azienda usa piani inferiori, il passaggio a Business Premium è quasi sempre il singolo intervento più efficiente sulla sicurezza, perché sblocca in un colpo solo la maggior parte degli strumenti citati in questo documento. Il livello avanzato può richiedere componenti aggiuntivi, come Entra ID P2 o Microsoft Sentinel, da valutare quando i fondamentali sono a posto.

Quanto al «chi fa cosa»: i livelli base e intermedio sono alla portata di un IT interno motivato, con tempo dedicato e una guida operativa come questa. Il livello avanzato — e soprattutto il presidio continuo di alert, log e risposta agli incidenti — è il punto in cui molte PMI scelgono un servizio gestito. In più di dieci anni al fianco delle PMI italiane, come SynSphere abbiamo visto funzionare entrambi i modelli: quello che non funziona mai è la via di mezzo, in cui la sicurezza è il compito di tutti e la responsabilità di nessuno.

10. Checklist operativa

La checklist che segue riassume l'intero framework in azioni concrete e verificabili. Usatela come strumento di lavoro, non come lettura: stampatela, spuntate ciò che è già a posto, assegnate un responsabile e una data a ciò che manca, e rivedetela a ogni trimestre.

Identità

- MFA attiva per il 100% degli utenti, senza eccezioni non documentate.
- Autenticazione legacy bloccata, con verifica nei log di accesso che nulla la usi ancora.
- Numero di amministratori globali ridotto al minimo, con account separati da quelli quotidiani.
- Due account break-glass creati, esclusi dal Conditional Access e monitorati a ogni utilizzo.
- Scadenza forzata delle password disattivata, protezione password di Entra ID attiva.

Posta elettronica

- SPF pubblicato e completo di tutte le sorgenti legittime di invio.
- DKIM abilitato su tutti i domini personalizzati del tenant.
- DMARC pubblicato, report analizzati ogni mese, policy portata a quarantine o reject.
- Preset security policy Standard (o Strict) applicata a tutti gli utenti.
- Protezione dall'impersonificazione configurata per dirigenti e partner critici.
- Inoltro automatico esterno bloccato e regole delle caselle auditate periodicamente.

Endpoint

- Dispositivi aziendali registrati in Intune con policy di conformità collegate al Conditional Access.
- Defender for Business attivo su tutti gli endpoint, regole ASR almeno in modalità audit.
- Update ring configurati e tasso di aggiornamento del parco macchine verificato ogni mese.
- BitLocker attivo su tutta la flotta, chiavi di ripristino custodite in Entra ID.
- App protection policy applicate ai dispositivi personali con accesso ai dati aziendali.

Dati

- Schema di etichette di riservatezza definito (3-4 etichette) e pubblicato agli utenti.
- Policy DLP per codice fiscale e IBAN attive, almeno in modalità monitoraggio.
- Policy di conservazione allineate agli obblighi legali e fiscali dell'azienda.
- Backup di Microsoft 365 attivo, con copie immutabili e ripristino granulare.
- Test di ripristino eseguito negli ultimi sei mesi, con esito verbalizzato.

Monitoraggio e risposta

- Secure Score rivisto ogni mese, con piano d'azione tracciato e decisioni documentate.
- Audit log attivo, con conservazione adeguata alle esigenze di conformità.
- Alert indirizzati a una casella o canale presidiato, con responsabile e priorità definiti.
- Piano di risposta agli incidenti scritto, stampato e distribuito alle persone giuste.
- Esercitazione tabletop svolta negli ultimi dodici mesi, con lezioni apprese a verbale.

Se a fine lettura la lista delle caselle vuote sembra lunga, è normale: nessun tenant parte perfetto, nemmeno quelli seguiti da specialisti. Quello che conta è l'ordine — identità, posta, endpoint, dati, monitoraggio — e la costanza con cui si procede. Sei mesi di lavoro ordinato su questa checklist trasformano la postura di sicurezza di una PMI molto più di qualsiasi prodotto comprato d'impulso dopo un incidente.

Chi è SynSphere

SynSphere Italia è un partner Microsoft specializzato nelle piccole e medie imprese italiane. Dal 2008 affianchiamo le aziende su Microsoft 365, Azure, Dynamics 365, sicurezza informatica e formazione, con sedi operative a Milano (Segrate) e Bolzano.

+150	**+10.000**	**0**
tenant Microsoft 365 gestiti	utenti migrati	downtime medio nelle migrazioni
+5.000	**+800**	**95%**
ore di formazione erogate	professionisti formati	soddisfazione dei corsi

Vuoi una mano sui temi di questo white paper? Parliamone: **synsphere.it/contattaci** · **info@synsphere.com**. Sul sito trovi anche strumenti gratuiti di assessment, toolkit PowerShell, template operativi e il catalogo completo di corsi e certificazioni Microsoft.