



CONTINUITY
SERVICE



HORNETSECURITY
BY proofpoint.

MIND THE GAP!

QUANDO L'EMAIL VA IN TILT, LA TUA
AZIENDA NON DOVREBBE FERMARSI.

LA VULNERABILITÀ NASCOSTA

La maggior parte delle aziende protegge i propri dati, ma dimentica di proteggersi dalle interruzioni delle comunicazioni. Colma il gap nascosto che può bloccare completamente l'operatività. Oggi ogni organizzazione investe in protezione dalle minacce, protezione dei dati, disaster recovery e conformità normativa. Ed è giusto così: sono elementi fondamentali.

MA COSA SUCCEDDE QUANDO IL SERVIZIO DI POSTA ELETTRONICA VA IN TILT?

Non a causa di un attacco informatico.

Non per errori interni.

Ma semplicemente perché il tuo provider email, come Microsoft 365, subisce un'interruzione.

In quel momento, tutto si ferma:

- » i commerciali non possono rispondere ai lead
- » il supporto non può aiutare i clienti
- » le operazioni si bloccano
- » le decisioni vengono rimandate
- » i ricavi iniziano a diminuire, minuto dopo minuto

QUESTO È IL COMMUNICATION GAP. ED È MOLTO PIÙ GRANDE DI QUANTO LA
MAGGIOR PARTE DELLE AZIENDE IMMAGINI.

LA REALTÀ: I DISSERVIZI SONO FREQUENTI, NON RARI

L'SLA di Microsoft 365 al 99,9% consente fino a 52 minuti di downtime all'anno, anche quando il servizio rispetta pienamente gli accordi.

E quando l'email si ferma, tutto si ferma: le vendite rallentano, il supporto si blocca, le decisioni si ritardano, la fiducia si perde. La vera domanda non è se la tua email smetterà di funzionare. La domanda è se sarai pronto quando accadrà.



METTE IN LUCE IL PROBLEMA

Secondo l'Articolo 21 della Direttiva NIS2, le organizzazioni devono dimostrare continuità operativa e capacità di gestione delle crisi, non solo documentarle.

IL GAP DI CONFORMITÀ CHE MOLTE ORGANIZZAZIONI NON CONSIDERANO:

- ✔ Esistono piani di disaster recovery
- ✔ Sono documentate procedure di risposta agli incidenti
- ✖ Nessuna soluzione per interruzioni parziali (es. outage di M365 di 6 ore o problemi regionali)
- ✖ Nessuna prontezza operativa mantenuta tra un incidente e l'altro

GLI AUDITOR **CHIEDERANNO:**

"COSA SUCCEDA DURANTE UN'INTERRUZIONE DEL PROVIDER?"

Senza un livello attivo di resilienza, la risposta resta solo teorica. E questo rappresenta un rischio di non conformità.

SOLUZIONE: CONTINUITY SERVICE DE HORNETSECURITY

Un livello strategico di resilienza operativa.

Continuity Service non è solo un backup email. È uno strumento di governance leggero che mantiene la tua organizzazione pronta tra una crisi e l'altra, garantendo la continuità operativa quando i sistemi principali falliscono.

PERCHÉ RISOLVE QUESTO GAP:

Basso sforzo, alto impatto

- » Nessuna infrastruttura da implementare
- » Nessun progetto complesso o fase pilota
- » Attivazione in pochi minuti tramite portale self-service
- » Configura una volta e mantieni automaticamente la prontezza operativa

Resilienza comprovata

- » 99,9% di disponibilità del servizio su infrastruttura indipendente
- » Failover automatico in pochi secondi (senza intervento manuale)
- » Archiviazione del traffico fino a 90 giorni
- » Supporto ai requisiti di conformità NIS2

Intelligenza operativa

- » Visibilità completa su tutte le email consegnate o in coda
- » Controllo amministrativo per attivare la continuità su tutto l'ambiente o su singole caselle
- » Sincronizzazione automatica quando il servizio principale torna operativo





COME FUNZIONA

DURANTE IL NORMALE FUNZIONAMENTO

Tutto il traffico email passa attraverso il provider principale (Microsoft 365, Exchange on-premise, ecc.). Continuity Service replica silenziosamente il traffico in background.

QUANDO SI VERIFICA UN'INTERRUZIONE

Il failover automatico si attiva immediatamente, senza alcuna azione da parte dell'IT.

- » Gli utenti accedono alla posta tramite interfaccia webmail sicura (POP3/IMAP disponibili)
- » Invio e ricezione continuano senza interruzioni
- » Tutte le email vengono archiviate fino a 90 giorni
- » Gli amministratori monitorano lo stato delle consegne in tempo reale

QUANDO IL SERVIZIO VIENE RIPRISTINATO

La sincronizzazione automatica reintegra tutte le email nel sistema principale.

- » Nessuna ricostruzione manuale
- » Nessuna conversazione persa
- » Nessuno stress da recupero

CONFRONTO DELL'IMPATTO

COSA VIENE COLPITO	SENZA CONTINUITY SERVICE	CON CONTINUITY SERVICE
Operatività email	Blocco totale durante il disservizio	Failover immediato, nessuna interruzione
Produttività del team	Ore o giorni di lavoro persi	Nessun downtime, il lavoro continua
Carico IT	Recupero manuale, stress, straordinari	Risincronizzazione automatica, nessun intervento manuale
Flusso operativo	Vendite, supporto e operazioni bloccati	Accesso continuo, operatività garantita
Conformità NIS2	Piani teorici	Resilienza dimostrabile, pronta per audit



PERCHÉ È IMPORTANTE ORA

IL COSTO DELLE INTERRUZIONI EMAIL

- » opportunità di vendita perse (interruzione dei cicli commerciali)
- » riduzione della soddisfazione dei clienti (i ticket di supporto si accumulano)
- » ritardi nelle decisioni interne
- » perdita di fiducia da parte dei clienti
- » rischio di non conformità normativa (la NIS2 richiede continuità dimostrabile)

IL VANTAGGIO STRATEGICO

Anche le migliori piattaforme cloud possono subire interruzioni. Continuity Service garantisce che non diventi interruzioni per il tuo business.

Le organizzazioni dotate di un livello attivo di continuità non solo si riprendono più velocemente, ma mantengono la prontezza operativa tra un incidente e l'altro, rafforzando nel tempo governance e resilienza.

L'ATTIVAZIONE È SEMPLICE

Puoi abilitare la continuità per:

- » tutto l'ambiente, oppure
- » singole caselle di posta critiche

Nessuna implementazione. Nessuna complessità. Solo resilienza operativa.

COLMA IL GAP PRIMA CHE TI COLPISCA

Continuity Service si attiva automaticamente in pochi secondi quando il tuo sistema email smette di funzionare.

NESSUNA INTERRUZIONE. NESSUN DOWNTIME.
NESSUNA OPPORTUNITÀ PERSA.

[RICHIEDI UNA DEMO](#)

