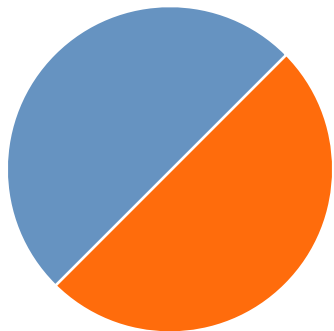
A hand is holding a white, cloud-shaped sticker with a cutout in the center. The background is a blurred laptop keyboard. The image is overlaid with a dark blue diagonal shape in the bottom right corner.

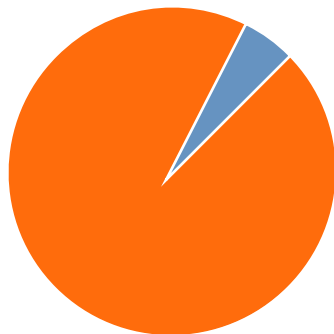
3 COSE DA
CONSIDERARE PRIMA
DI TRASFERIRE LA
POSTA ELETTRONICA SU
MICROSOFT OFFICE 365

Il passaggio al cloud

Le organizzazioni stanno cogliendo l'utilità di trasferire nel cloud i servizi e le applicazioni aziendali, e la posta elettronica è uno dei primi servizi a subire questo passaggio. Non stupisce che aziende di ogni dimensione scelgano sempre più spesso Microsoft Office 365. Per potenziare le caratteristiche di sicurezza native di Office 365, molte aziende stanno anche valutando una soluzione di sicurezza e-mail basata su cloud.



Entro il 2020, il 50% delle aziende si affiderà a strumenti di sicurezza non Microsoft¹



Il 95% dei clienti nuovi o in transizione cerca soluzioni di e-mail security basate sul cloud²

1. Report di Gartner: [How to Enhance the Security of Office 365](#)

2. Report di Gartner: [Market Guide for Secure Email Gateways](#)



Compare Exchange Online plans

\$4.00 per month
(annual commitment)

Exchange Online Plan 1

Buy now

\$8.00 per month
(annual commitment)

Exchange Online Plan 2

Buy now

\$12.00 per month
(annual commitment)

Office 365

1 year \$12.00 per user

Scegliere il giusto piano di Office 365

Le aziende che decidono di trasferire il proprio servizio di posta elettronica in Office 365 devono individuare il piano di Exchange Online che fornisca il valore più adatto alla propria attività.



Colmare le lacune

Integrando servizi aggiuntivi in abbonamento per soddisfare tutti i casi d'uso in azienda (ad es. protezione dalle minacce avanzate), i risparmi legati al trasferimento nel cloud possono svanire in fretta.

3 cose da considerare



Protezione
contro le minacce
avanzate

Spear Phishing
Ransomware
Business Email Compromise
Frodi via e-mail



DLP e
conformità

Normative di settore
Norme nazionali
Perdite di dati



Continuità
della posta
elettronica

Interruzioni del servizio
Tempi di fermo per
manutenzione

Protezione contro le minacce avanzate

- Office 365 offre Exchange Online Protection (EOP), che include antispam e antimalware
- Ma per fermare ransomware, attacchi di phishing mirato e business email compromise (BEC) servono funzionalità di protezione contro le minacce avanzate

Il servizio Office 365 Advanced Threat Protection (ATP) è incluso solo nei piani più avanzati (EOP 5 e superiore). I piani di livello inferiore richiedono l'acquisto di ATP come servizio supplementare a costi aggiuntivi.



Conformità DLP

- La posta elettronica è essenziale per le imprese e spesso include dati sensibili come informazioni sulle transazioni commerciali, IP aziendale, dati sulle vendite e/o sui clienti e tanto altro ancora
- Le norme nazionali e le normative di settore impongono alle organizzazioni di garantire la conformità delle proprie comunicazioni e-mail agli standard vigenti
- I responsabili IT devono riconsiderare il rischio di perdite di dati e le problematiche di conformità nei propri server di posta nel cloud

I piani di Microsoft Office 365 includono funzioni di prevenzione della perdita di dati (DLP) e di conformità nella versione premium per le imprese, ma nelle versioni per le PMI offrono funzionalità limitate, creando potenziali falle in termini di sicurezza e a livello giuridico.



Continuità della posta elettronica

- Con il passaggio a Office 365, alcuni amministratori IT potrebbero trascurare la pianificazione necessaria a garantire la continua operatività dell'infrastruttura locale
- Tutti i servizi cloud sono soggetti a interruzioni, proprio come le soluzioni locali. Se Exchange Online dovesse subire un'interruzione, gli utenti finali se ne accorgerebbero immediatamente.
- Un'interruzione di Office 365 non è solo una seccatura. Può comportare nuovi rischi per la sicurezza, nel momento in cui gli utenti ricorrono all'e-mail personale per mantenere la produttività

Microsoft offre accordi sul livello dei servizi con un valore pari al 99,9%, ma Office 365 subisce delle interruzioni. Quando questo accade, ai clienti viene riconosciuta una qualche forma di rimborso. Ma che dire della produttività perduta e del potenziale impatto sull'attività aziendale derivante dalle mancate vendite? Una PMI può raramente permettersi un tale impatto.



The background is a collage of financial and navigational symbols. On the left, there are several tall stacks of silver coins. In the center and right, there are individual coins scattered, including a 2 Euro coin and a 1 Euro coin. A compass rose is visible in the upper right quadrant. Overlaid on the entire scene are several thin, glowing lines in white, yellow, and red, resembling a stock market line graph or data visualization.

Sostenibilità economica

L'acquisto di più servizi necessari per la sicurezza, la conformità e la continuità può rivelarsi presto dispendioso, rendendo Office 365 una prospettiva meno vantaggiosa, di poco risparmio o persino più onerosa per via dei costi nascosti.

Conclusioni

La posta elettronica resta il principale vettore di minacce per le imprese. Oltre il 90% delle violazioni dei dati parte da un'e-mail, il che sottolinea la necessità che le aziende investano in best practice e funzionalità di sicurezza.

Un sistema di protezione della posta elettronica avanzato deve avere un approccio multilivello e combinare più soluzioni per proteggere al meglio dalle minacce in continua evoluzione.

La soluzione Hosted Email Security (HES) di SonicWall aiuta a realizzare i risparmi derivanti dall'adozione di Microsoft Office 365 offrendo le migliori funzionalità di protezione contro le minacce avanzate, prevenzione della perdita di dati, conformità e continuità della posta elettronica.

Leggi il nostro documento tecnico per scoprire come SonicWall HES garantisce la continuità della posta elettronica



CONTATTACI
per richiedere una demo

The diagram illustrates the SonicWall Capture Labs security stack. At the top is the 'CAPTURE LABS' logo, which features a stylized atom symbol. Below the logo is a yellow banner with the text 'Feed di intelligence contro le minacce in tempo reale'. The main body of the stack consists of five dark blue horizontal bars, each containing an icon and a security feature name: 1. A shield with a checkmark icon for 'Advanced Threat Protection'. 2. A fedora hat icon for 'Anti-Spoofing'. 3. A computer keyboard icon for 'Anti-Phishing'. 4. A shield with an 'X' icon for 'Anti-Virus & Anti-Spam'. 5. A folder with a lock icon for 'DLP & Compliance'. At the bottom of the stack is an orange banner with the text 'OPZIONI DI IMPLEMENTAZIONE: IN SEDE | VIRTUALE | CLOUD'.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

© 2018 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. SALVO QUANTO SPECIFICATO NEI TERMINI E NELLE CONDIZIONI STABILITI NEL CONTRATTO DI LICENZA DI QUESTO PRODOTTO, SONICWALL E/O LE SUE AFFILIATE NON SI ASSUMONO ALCUNA RESPONSABILITÀ ED ESCLUDONO GARANZIE DI QUALSIASI TIPO, ESPLICITE, IMPLICITE O LEGALI, IN RELAZIONE AI PROPRI PRODOTTI, INCLUSE, IN VIA ESEMPLIFICATIVA, QUALSIASI GARANZIA IMPLICITA DI COMMERCIALIZZABILITÀ, IDONEITÀ A SCOPI SPECIFICI O VIOLAZIONE DI DIRITTI ALTRUI. SONICWALL E/O LE SUE AFFILIATE DECLINANO OGNI RESPONSABILITÀ PER DANNI DI QUALUNQUE TIPO, SIANO ESSI DIRETTI, INDIRETTI, CONSEGUENZIALI, PUNITIVI, SPECIALI O INCIDENTALI (INCLUSI, SENZA LIMITAZIONI, DANNI PER MANCATO GUADAGNO, INTERRUZIONI DELL'ATTIVITÀ O PERDITE DI DATI) DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE DOCUMENTO, ANCHE NEL CASO IN CUI SONICWALL E/O LE SUE AFFILIATE SIANO STATE AVVERTITE DELL'EVENTUALITÀ DI TALI DANNI. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riserva il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.