Avira Exchange Security

Comunicazione sicura: gestione centralizzata delle email con Avira

Protezione in tempo reale da virus e phishing

Protezione da virus, file allegati indesiderati ed email di phishing

Rilevamento di email di phishing

Scansione periodica dei virus per tutte le email e i file allegati in tempo reale, programmata e

E basata sul calcolo degli eventi Rilevamento degli allegati mediante modelli di file univoci e non manipolabili (impronte digitali)

Creazione e uso di impronte digitali specifiche per l'azienda

Definizione delle restrizioni sui file mediante la combinazione di nome, estensione e dimensioni del file

Applicazione delle restrizioni sui file agli archivi, ad esempio ZIP e RAR

Tecnologia di rilevamento basata su cloud per per proteggersi da attacchi sconosciuti (exploit zero-day)

Protezione a più livelli da spam, analisi intelligente del contenuto

Potente tecnologia antispam

Gestione centralizzata della quarantena con diritti di accesso specifici per utenti

Blocco delle email provenienti da mittenti non desiderati

Gestione di whitelist e blacklist sul server specifica per utenti

Verifica centralizzata di email crittografate

Notifiche flessibili delle email bloccate agli amministratori o ai destinatari/mittenti

Verifica di contenuti vietati, indesiderati o sensibili secondo le direttive aziendali

La maggior parte dei processi aziendali ha successo solo se la comunicazione via email non presenta difficoltà. Se la comunicazione viene disturbata, si verificano ritardi che comportano costi notevoli. Sono da aspettarsi conseguenze più gravi se gli hacker utilizzano allegati di posta elettronica appositamente preparati per penetrare nella rete e nelle banche dati, perché ciò mette in pericolo il funzionamento dell'impresa. Se l'azienda inoltra email infette non rilevate a clienti o partner commerciali, ciò è non solo spiacevole ma anche pericoloso, in quanto tutti gli interessati possono essere danneggiati.

Con **Avira Exchange Security**, le aziende possono contare su un sistema di protezione altamente efficiente senza compromettere le prestazioni dell'infrastruttura di scambio o i processi in esecuzione. Gli allegati pericolosi vengono riconosciuti e bloccati in modo efficace. I tentativi di phishing e spamming vengono respinti all'istante.

Avira Exchange Security: modalità di funzionamento

Server di posta in arrivo →

- Email commerciali e riservate
- Email con allegati dannosi
- Email con allegati di dimensioni eccessive
- phishing
- Spam
- Email spazzatura

Avira Antivirus e AntiSpam →

- Gli allegati vengono bloccati
- I contenuti vengono analizzati
- I contenuti vengono filtrati

- Quarantena
- Categorizzazione
- Notifica

Risultato

- Email prive di virus, allegati sicuri
- Nessun fastidio causato dalla spam
- Messaggi di posta elettronica suddivisi per categorie
- Panoramica del traffico email e degli eventi
- Possibilità di protocollo e di gestione

Avira Exchange Security

Comunicazione sicura: gestione centralizzata delle email con Avira

Requisiti di sistema e rilascio licenze

Microsoft Exchange Server
Microsoft Exchange Server 2007 (64 bit), compresi gli ultimi aggiornamenti cumulativi

Microsoft Exchange Server 2010 (64 bit), compresi i Service Pack fino a SP2 ei relativi aggiornamenti cumulativi

Microsoft Exchange Server 2013 (64 Bit) su Windows Server 2012 (Avira Exchange Security installato su "Mailbox Server")

Microsoft Exchange Server 2016

Sistemi operativi
Windows Server 2008 R2 (compresi i Service Pack e le patch aggiornati)

Windows Server 2012 (64 Bit)

Windows Server 2012 R2 (64 Bit)

RAM
quella consigliata per Exchange + ulteriori 64 MB

HDD
Minimo 400 MB

Extra
Drive CD-ROM o accesso di rete,

Microsoft .NET Framework 3.5 plus 4.0 .NET Framework Client Profile

Raccomandati 100 MB per la registrazione degli eventi, connessione a Internet necessaria

Prezzi delle licenze
Intesi per ciascun dispositivo protetto. Durata delle licenze: 1, 2 o 3 anni

La licenza comprende
Aggiornamenti e upgrade gratuiti per tutto il periodo di validità

Software da scaricare
Avira Gold Support

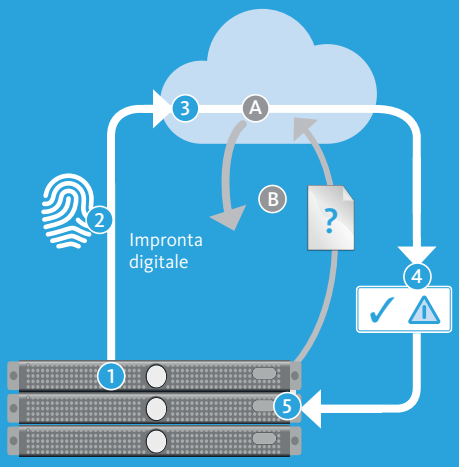
1. Avira Exchange Security riconosce un file sospetto allegato ad un'email.
2. L'impronta digitale del file viene trasferita ad Avira Protection Cloud per essere analizzata.
3. Questa impronta digitale viene confrontata con i file precedentemente scansionati da Protection Cloud. Questo può portare a due risultati:

A. l'impronta digitale appartiene a un file già controllato da Protection Cloud che viene classificato come sicuro o come malware.

B. Oppure Avira Protection Cloud non conosce ancora questa impronta digitale. Protection Cloud carica il file, lo analizza e lo classifica come sicuro o come malware.

4. Avira Protection Cloud segnala quindi lo stato dell'impronta digitale (sicura o infetta) ad Avira Exchange Security.
5. Nel caso in cui il file venga classificato come malware, Avira Exchange Security elimina il pericolo.

Avira Protection Cloud



Ulteriori informazioni su Avira Protection Cloud sono disponibili su:
http://www.avira.com/it/avira-protection-cloud

Avira Protection Cloud: protezione online intelligente per le aziende

Avira Protection Cloud è la risposta alle minacce sempre più complesse provenienti da virus e cyber-criminali: rileva le minacce in tempo reale e le elimina con successo. Grazie a una tecnologia avanzata costituita da moduli di riconoscimento dei file di ultima generazione, funzioni convesse e intelligenza artificiale, utilizza una piattaforma di sicurezza online globale attiva 24 ore su 24, che si basa su una rete di svariati milioni di computer. In una frazione di secondo i file vengono esaminati e classificati in modo affidabile come "sicuri" o "infetti".

Oltre alla sicurezza nettamente superiore e al breve tempo di risposta, Avira Protection Cloud offre un altro vantaggio: necessita di pochissima memoria locale. Avira Protection Cloud è facile da utilizzare e sempre aggiornato. Inoltre, si integra perfettamente nei sistemi esistenti.