

Kaspersky Endpoint Security Cloud

Nome, posizione

kaspersky

Una pericolosa illusione

Le PMI credono:

"Siamo troppo piccoli per diventare un bersaglio dei cybercriminali".



Statistiche reali:

Il 50%

delle violazioni legate ad attacchi informatici è stato effettuato da gruppi criminali organizzati*

Il 58%

delle vittime fa parte della categoria aziende di piccole dimensioni**

Il 60%

delle piccole e medie imprese violate da attacchi hacker cessa le proprie attività di business entro sei mesi***

Le sfide per l'amministratore IT nelle PMI

Sono sommerso di lavoro

Il 66%

delle aziende dichiara che la gestione di un ambiente IT eterogeneo rappresenta la principale sfida.

Risorse e budget sono limitati

Il 66%

delle PMI gestisce la sicurezza come parte di più ampie esigenze IT, senza competenze dedicate in materia di sicurezza informatica.



La forza lavoro che opera da remoto è un rischio per la sicurezza

Il 40%

delle PMI consente regolarmente ai propri dipendenti di lavorare da remoto, al di fuori del perimetro aziendale.

Il 50%

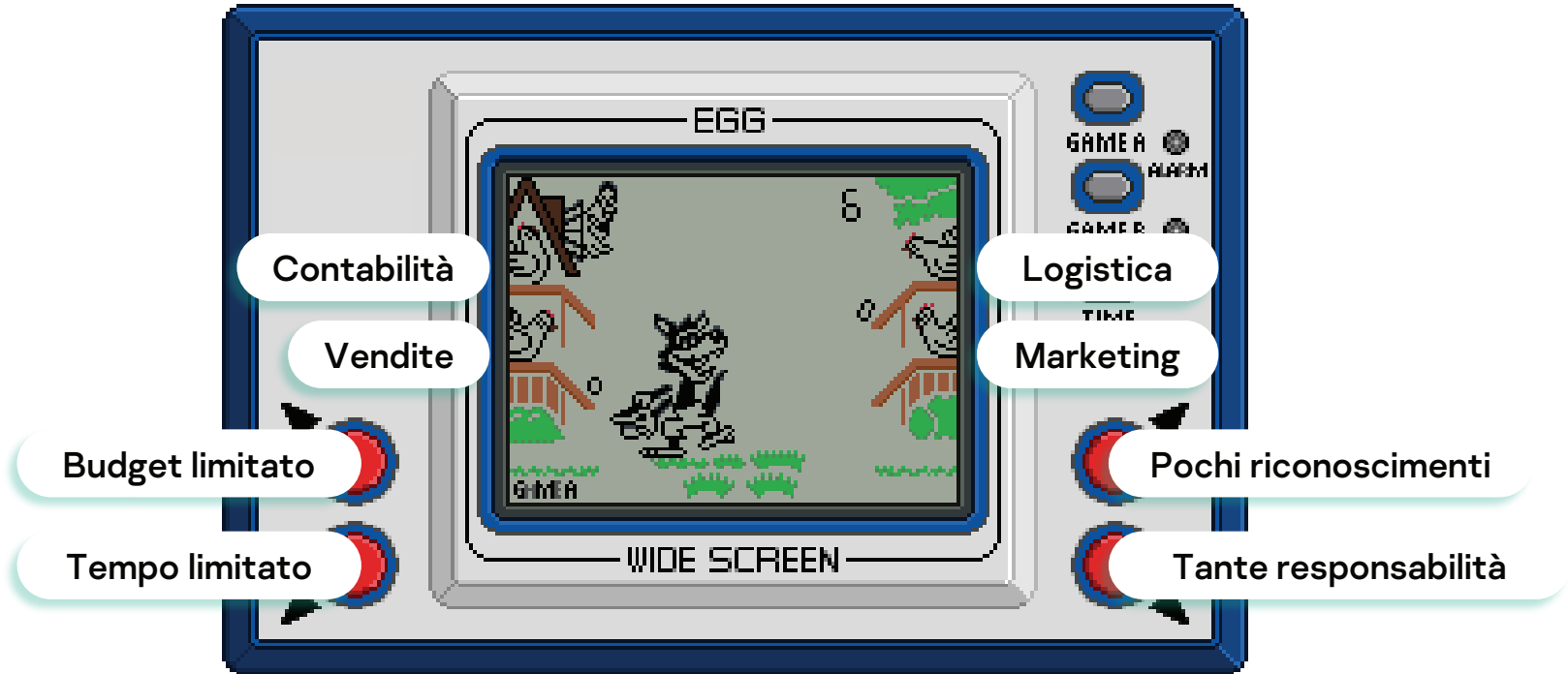
dei dipendenti utilizza nel lavoro dispositivi personali, compresi i dispositivi mobili.

Il 64%

delle PMI memorizza le informazioni sensibili dei clienti sui dispositivi mobili dei dipendenti.

Giornata di lavoro tipo di un amministratore IT...

4



Il modo più semplice per proteggere l'azienda, senza compromettere risorse IT, tempo o budget



Protezione per qualsiasi dispositivo

- Desktop e laptop Windows/Mac
- File server Windows
- Smartphone e tablet Android/iOS



Diminuzione del carico di lavoro generato dalla gestione on-premise

- Soluzione cloud-based, sempre disponibile su cloud.kaspersky.com
- Console intuitiva, gestibile tramite un browser web



Ottimizzazione dei costi

- Disponibile con subscription mensile
- Scelta tra due livelli di prezzo:
 - Kaspersky Endpoint Security Cloud
 - Kaspersky Endpoint Security Cloud Plus



Kaspersky Endpoint Security Cloud assicura

- Protezione in tempi più rapidi
- Nessun investimento di capitale
- Niente più patch cumulative da eseguire il venerdì
- Ridistribuzione delle risorse
- Più tempo per le attività business-critical



**Protezione leader
per il settore
delle PMI.**

- Tecnologie di protezione endpoint dal vendor di soluzioni di sicurezza IT più premiato e testato.



**Soluzione
automatizzata per
ridurre i costi IT e
liberare risorse.**

- Nessun provisioning di hardware e software. È sufficiente registrarsi su cloud.kaspersky.com.
- Protezione pronta all'uso con policy predefinite sviluppate dai nostri esperti di sicurezza.



**Protezione dei
dipendenti che
operano da remoto,
ovunque si trovino.**

- Gestione degli utenti remoti tramite console cloud-based e applicazione da remoto dei criteri di sicurezza.
- Per ogni utente due licenze per dispositivi mobili gratuite.

Kaspersky Endpoint Security Cloud

7

Kaspersky ha ottenuto più primi posti in test indipendenti rispetto a qualsiasi altro vendor di soluzioni di sicurezza.

E i riconoscimenti continuano ad arrivare anno dopo anno.



**PROTEZIONE KASPERSKY
LA PIÙ TESTATA*
LA PIÙ PREMIATA***

[*kaspersky.com/it/top3](https://kaspersky.com/it/top3)

86

Test/recensioni

81%

TOP3

64

Primi posti





Protezione

- Protezione su file, e-mail e web, per un'efficace difesa dalle minacce malware note, sconosciute e avanzate
- Exploit prevention e anti-ransomware per monitorare le applicazioni vulnerabili
- Remediation engine, per eseguire il rollback dei danni provocati dai cryptolocker
- Firewall per bloccare le connessioni di rete non autorizzate
- Vulnerability assessment con raccomandazioni sull'applicazione delle patch o sul patch management integrato



Gestione della sicurezza e controlli

- Cloud Discovery
- Protezione per Microsoft Office 365
- Web Control
- Device Control
- Patch Management
- Gestione della crittografia



Sicurezza dei dispositivi mobili

- Antivirus per dispositivi mobili
- Gestione delle password
- Web Control e controllo funzionalità
- Funzionalità antifurto

Soluzione pronta all'uso

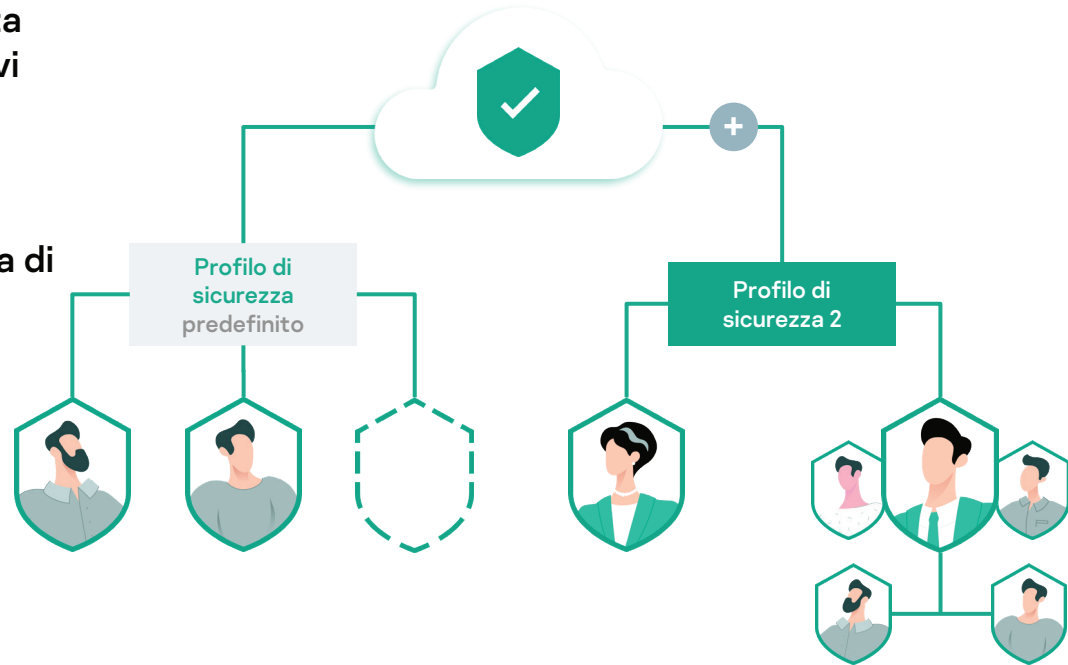
Tutto ciò che occorre è un browser e una connessione a Internet



Profilo di sicurezza user-based

10

- Un singolo profilo di sicurezza associabile a tutti i dispositivi dell'utente
- Create fino a **20** profili aggiuntivi associabili a dispositivi diversi in ogni area di lavoro per personalizzare il livello di protezione



Tenete sotto controllo i dispositivi mobili non gestiti

11

Protezione mobile antivirus e web

- Protezione in tempo reale da minacce, virus e applicazioni malevole
- Blocco dei siti web di phishing e dannosi

Gestione delle password

- Applicazione della password di sblocco dello schermo
- Supporto per Face ID e Touch ID

Funzionalità antifurto da remoto

- Localizzazione/blocco del dispositivo
- Attivazione di un allarme
- Cancellazione dei dati

Mobilità per il lavoro, non per il divertimento

- Application Control per Android
- Controllo funzionalità

Funzionalità complete per dispositivi iOS supervisionati

- Web Control
- Impostazioni proxy
- Limitazioni delle funzionalità (fino a 40 funzionalità)

Il **61%** delle PMI si dichiara d'accordo o fortemente d'accordo sul fatto che l'azienda debba incoraggiare e premiare la collaboration.

Il **70%** delle piccole imprese si dichiara d'accordo o fortemente d'accordo sul fatto che le soluzioni adottate in azienda in termini di comunicazione e collaboration contribuiscano a migliorare il livello di produttività.

Solo il **38%** degli acquisti in ambito tecnologico è attualmente gestito, definito e controllato dai responsabili aziendali.

"...i dipendenti utilizzano facilmente soluzioni di collaboration non autorizzate, che possono creare problemi a livello di supporto e notevoli rischi per la sicurezza."

Cosa stanno effettivamente facendo gli utenti con i servizi cloud?

13

Chattano tramite applicazioni di messaggistica web

Perdono tempo prezioso sui social network

Condividono i dati aziendali su cloud personali



Diminuzione della produttività

Nessuna visibilità riguardo all'effettivo utilizzo del cloud

Nessun tipo di controllo sui dati presenti nel cloud

Non è chiaro quali siano le dinamiche dei flussi dell'intero traffico aziendale



La prima soluzione per la discovery di scenari Shadow IT economicamente vantaggiosa

- Endpoint-based
- Nessuna procedura di deployment
- Nessuna implementazione
- Si attiva con pochi, semplici clic

Analisi dell'utilizzo del cloud

- Dashboard
- Widget
- Report

Applica le necessarie restrizioni tramite

- Blocco degli utenti
- Blacklisting dei servizi indesiderati
- Blocco di determinate categorie

Include Kaspersky Security for Microsoft Office 365

Una volta combattuto con efficacia lo Shadow IT grazie a Cloud Discovery, si può implementare in tutta sicurezza Microsoft Office 365 con la nostra protezione già inclusa in Kaspersky Endpoint Security Cloud Plus



Protezione all-in-one per tutti i principali servizi di comunicazione e collaboration della suite O365.

- Blocca phishing e Business Email Compromise (BEC), per impedire i furti di account
- Previene la diffusione del malware veicolato tramite e-mail e cloud storage aziendale
- Blocca i più sofisticati metodi di spam
- Rimuove gli allegati indesiderati prima che l'utente possa commettere un errore

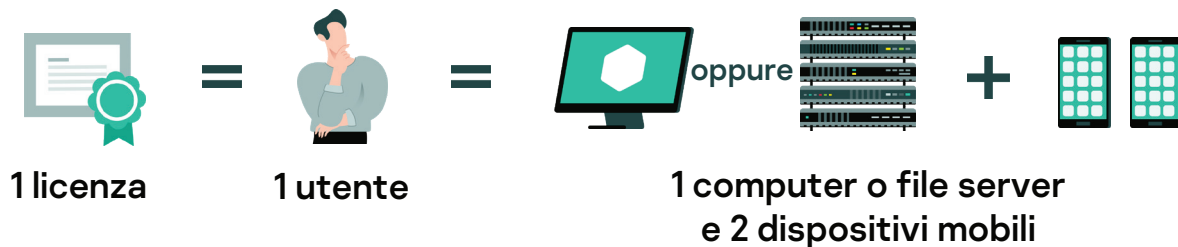
Nessuna necessità di software aggiuntivo o ulteriori server:

Provate le funzionalità di gestione su [Kaspersky Business Hub](#)

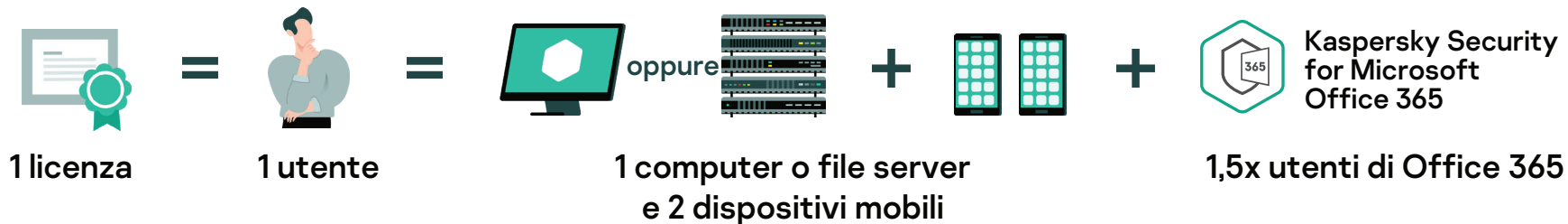
Nessun ritardo introdotto nell'elaborazione delle e-mail.

Integrazione completa con Microsoft Office 365 tramite API e utilizzo dei workload di Microsoft Azure.

1. Acquistando **Kaspersky Endpoint Security Cloud**



2. Acquistando **Kaspersky Endpoint Security Cloud Plus**



Kaspersky Endpoint Security Cloud copre la maggior parte delle raccomandazioni contenute nella "Cyber Security: Small Business Guide", pubblicata dal National Cyber Security Centre, Regno Unito

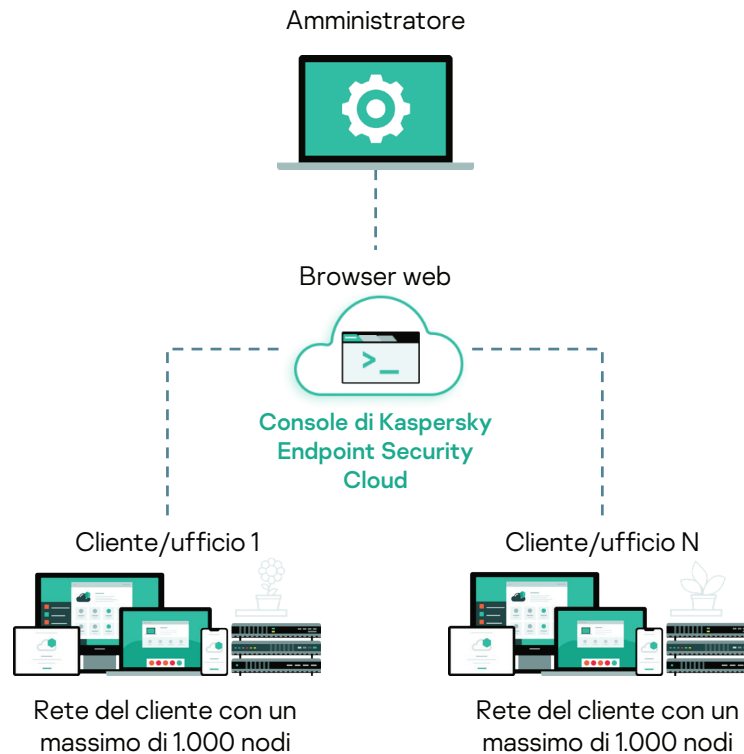
- ✓ Installare e attivare il software antivirus
- ✓ Attivare il firewall
- ✓ Attivare la protezione tramite password
- ✓ Mantenere aggiornate le applicazioni
- ✓ Mantenere aggiornato il dispositivo
- ✓ Mantenere aggiornate tutte le apparecchiature IT (applicazione di patch)
- ✓ Controllare come si possono utilizzare le unità USB
- ✓ Implementare restrizioni per impedire agli utenti il download di applicazioni di terze parti
- ✓ Installare e attivare applicazioni di monitoraggio per tutti i dispositivi in uso, ad es. Trova il mio iPhone

Console multi-tenancy

- Agevola il compito degli MSP (Managed Service Provider) nel soddisfare le esigenze di sicurezza di numerosi clienti, da remoto e senza aggiungere complessità.
- Semplifica la gestione della sicurezza per le aziende con più uffici dislocati geograficamente

Co-gestione dell'endpoint security

- Consente di creare più amministratori per ogni area di lavoro.
- Consente di visualizzare diverse aree di lavoro in un'unica finestra della console, per gestire più organizzazioni.
- Per un MSP è possibile collegare gli amministratori esterni o del cliente per le attività di co-gestione



Licenze flessibili

La soluzione Security-as-a-Service è il connubio perfetto che unisce il fai da te e i servizi professionali o gestiti.

L'offerta automatizzata è interessante perché assicura convenienza e può compensare la mancanza di risorse IT e/o di tempo.

Vantaggi di Kaspersky Endpoint Security Cloud

- Protezione in tempi più rapidi
- Nessun investimento di capitale
- Server gratuito per la redistribuzione relativa ai task business-critical
- Sempre la versione più recente e aggiornata del prodotto
- Niente più patch cumulative per il server da eseguire il venerdì
- Gestione da qualsiasi luogo con la console web
- Tempo da dedicare ai task business-critical
- Maggiore produttività dei dipendenti



**Kaspersky
Endpoint Security
Cloud**

Interfaccia web su misura per amministratori IT molto impegnati

20

Kaspersky Endpoint Security Cloud
St Mary Hospital

Getting started | **Monitoring** | Reports | Event log | License

Widgets

Each widget contains information about all managed devices. Unless otherwise specified, widgets show information from the last 30 days.

Cloud Discovery

Cloud Discovery allows you to monitor cloud services that are used most often on Windows devices in your company. Cannot find a cloud service that your company uses? [Let us know](#)

Cloud Discovery information

6760	Miscellaneous
2524	Social Media
977	File sharing
185	Messengers
69	Email

TOP 5 services

6241	Salesforce
237	Zoho
75	Acumatica
73	Office 365
59	Yammer

Select a category of cloud services to view the five services most often used from this category. Select a specific service to view users who most often access the service.

Protection

Widgets in this section provide you with information about the protection status of managed devices.

Protection status of devices

6	OK
0	Warning
0	Critical

Status of anti-virus database updates

5	During last 24 hours
1	During last 3 days
0	During last 7 days
0	More than a week ago

Privacy Policy
Legal Notice
Help
Support

© 2019 AO Kaspersky Lab. All Rights Reserved.

Le due versioni a confronto

	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security Cloud Plus
FUNZIONALITÀ DI SICUREZZA		
File, Web e Mail Threat Protection	✓	✓
Firewall	✓	✓
Network Attack Blocker	✓	✓
Exploit prevention e anti-ransomware	✓	✓
Vulnerability assessment	✓	✓
Discovery di servizi cloud novità	✓	✓
FUNZIONALITÀ DI GESTIONE		
Blocco servizi cloud novità		✓
Protezione per Microsoft Office 365 novità		✓
Web Control		✓
Device Control		✓
Gestione della crittografia		✓
Patch Management		✓

Extra livello Plus:

Discovery e blocco dei servizi cloud **Novità**

Riduzione del numero di servizi IT cloud non controllati nell'ambito della rete aziendale.

Protezione per Microsoft Office 365 **Novità**

Protezione avanzata dalle minacce per le applicazioni Exchange Online, OneDrive, SharePoint Online e Teams.

Device Control

Controllo dell'accesso degli utenti a dispositivi rimovibili ed esterni collegati al computer.

Web Control

Controllo dell'accesso degli utenti a Internet, secondo variabili quali la posizione o il contenuto del sito.

Patch Management

Gestione da remoto degli aggiornamenti e delle patch per le applicazioni installate sui dispositivi aziendali.

Gestione della crittografia

Crittografia da remoto sui dispositivi dei dipendenti tramite il componente nativo Windows Encryption (BitLocker) e Mac OS (FileVault).

Let's talk?

Sede centrale di Kaspersky Italia
Via Francesco Benaglia 13,
00153 Roma, Italia
Tel.: +39 06 5814168
www.kaspersky.it

kaspersky