



## Kaspersky® Endpoint Security for Business

Advanced



Ready  
for GDPR

**Kaspersky Endpoint Security for Business Advanced** combina una protezione multilivello con strumenti di controllo avanzati, per offrire una soluzione di sicurezza flessibile che si adatta rapidamente alle nuove minacce. La console centralizzata di gestione dei sistemi e della sicurezza garantisce la massima efficienza, mentre i livelli aggiuntivi di difesa aiutano a eliminare le vulnerabilità e a proteggere i dati sensibili.

### Le funzionalità di protezione e gestione di cui avete bisogno

Kaspersky Lab ha sviluppato strumenti e tecnologie di classe Enterprise attraverso livelli progressivi. Abbiamo fatto in modo che la tecnologia fosse flessibile e di facile utilizzo per aziende di qualsiasi dimensione.

#### Qual è la versione più adatta a voi?

- SELECT
- **ADVANCED**
- TOTAL

#### Più livelli di protezione per

- Windows, Linux e Mac
- Server Windows e Linux
- Container Windows Server
- Android e altri dispositivi mobili
- Dispositivi rimovibili

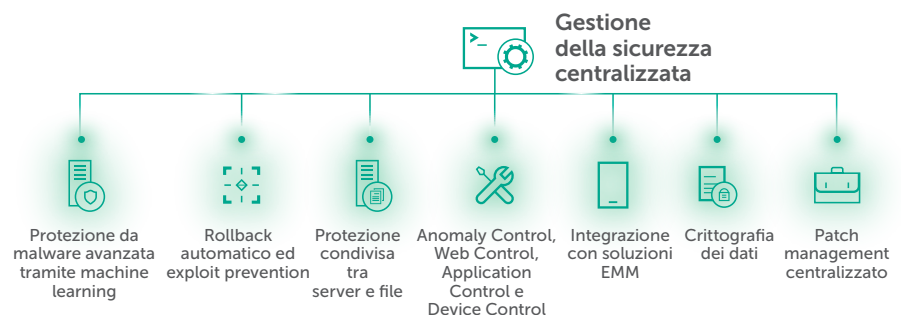
#### Protezione senza precedenti da

- Exploit del software
- Ransomware
- Malware per piattaforme mobile
- Minacce avanzate
- Minacce fileless
- PowerShell e altri attacchi basati su script
- Minacce sul web

#### Funzionalità incluse

- Anti-malware livello successivo
- Gestione delle vulnerabilità
- Security Policy Adviser
- Apprendimento basato su IA
- Supporto di AMSI novità
- Scansione del traffico crittografato novità
- Process isolation
- Exploit prevention e rollback
- Gestione del firewall e di quello del sistema operativo
- Protezione assistita da cloud
- Agente EDR integrato
- Adaptive Anomaly Control novità
- Application Control, Web Control e Device Control
- Protezione di server e container livello successivo
- Protezione dei server terminal
- Supporto del sottosistema Windows per Linux novità
- Mobile Threat Defense livello successivo
- Gestione della crittografia del sistema operativo
- Setup e configurazione del sistema
- Patch management livello successivo
- Creazione di report

Per i dettagli, visitate le nostre pagine web [qui](#).



## Funzionalità flessibili per proteggere i dati

### Unica console di gestione

Dalla console di gestione centralizzata, gli amministratori hanno visibilità e controllo su tutte le scelte di sicurezza applicate a ogni singolo endpoint nell'azienda. Questo consente la massima semplicità di setup e gestione con il minimo sforzo, utilizzando la vasta gamma di scenari preconfigurati.

### Sicurezza flessibile e adattabile

Il prodotto è ideato per funzionare in qualsiasi ambiente IT, utilizzando un set completo di tecnologie NextGen comprovate per prevenire gli attacchi rilevati; i sensori incorporati e l'integrazione con Kaspersky Endpoint Detection and Response (EDR) consentono di acquisire grandi volumi di dati per identificare i cyberattacchi più avanzati e sofisticati.

### Un unico prodotto, costi trasparenti

Con molteplici tecnologie di sicurezza integrate in un singolo prodotto, non esistono costi nascosti. Una licenza equivale a un prodotto, e tutte le funzionalità necessarie sono al suo interno.

### Soddisfazione del cliente garantita

La grande attenzione rivolta al dipartimento R&D ci spinge a sviluppare prodotti in grado di garantire la sicurezza di cui avete bisogno. I decision-maker esprimono costantemente enorme soddisfazione per i risultati ottenuti, come confermato nei report e nei sondaggi indipendenti.

# Funzionalità principali

## Strumenti di controllo degli endpoint cloud-enabled

### Funzionalità Anomaly Control e Application Control uniche

L'Adaptive Anomaly Control, che adatta automaticamente la sicurezza al massimo livello appropriato a ciascun ruolo nell'organizzazione, è completata dal modulo Application Control di livello Enterprise e da un database di whitelisting sempre aggiornato.

### Host Intrusion Prevention System (HIPS)

Regola l'accesso ai dati sensibili e ai dispositivi di registrazione utilizzando i reputation database locali ed in cloud (Kaspersky Security Network), senza influire sulle performance delle applicazioni autorizzate.

### Device Control, Web Control e molto altro...

## Crittografia e protezione dei dati

### Crittografia completa

Il security team può applicare centralmente la crittografia con certificazione FIPS 140.2 e Common Criteria (a livello di file, disco o dispositivo) e gestire gli strumenti di crittografia nativa come Microsoft BitLocker e macOS FileVault.

### Criteri integrati e unificati

L'esclusiva integrazione della crittografia con Application Control e Device Control fornisce un livello aggiuntivo di sicurezza e praticità di amministrazione.

## Funzionalità essenziali di protezione dalle minacce

### Analisi comportamentale e rollback automatico

Assicura il rilevamento e la protezione da minacce avanzate, tra cui ransomware, attacchi fileless e furti degli account di amministrazione. L'analisi comportamentale consente di bloccare gli attacchi, mentre il rollback automatico annulla le modifiche già apportate.

### Protezione contro la crittografia delle cartelle condivise

Un unico meccanismo "anti-cryptor" è in grado di impedire ai processi dannosi eseguiti su altre macchine nella stessa rete di crittografare i file archiviati su risorse condivise.

### Protezione per container e server terminal

Protegge i container basati su Windows Server e una vasta gamma di ambienti di accesso da remoto, tra cui Microsoft Remote Desktop Services e Citrix XenApp/Xen Desktop. Il componente per la sicurezza del traffico fornisce protezione per il web e il traffico di posta elettronica sul server terminal.

Kaspersky Lab

Trovate il partner più vicino: [www.kaspersky.com/buyoffline](http://www.kaspersky.com/buyoffline)

Kaspersky for Business: [www.kaspersky.com/business](http://www.kaspersky.com/business)

Novità sulla sicurezza IT: [business.kaspersky.com/](http://business.kaspersky.com/)

Il nostro approccio unico: [www.kaspersky.it/true-cybersecurity](http://www.kaspersky.it/true-cybersecurity)

#truecybersecurity  
#HuMachine

[www.kaspersky.it](http://www.kaspersky.it)

© 2019 AO Kaspersky Lab. Tutti i diritti riservati. I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.

## Exploit prevention, neutralizzazione dei rootkit e altro ancora...

## Funzionalità di Mobile Threat Defense

### Tecnologie anti-malware innovative

Combinazione del rilevamento assistito da cloud, proattivo e basato su machine learning con protezione in tempo reale. La protezione web e le scansioni on-demand e pianificate aumentano la sicurezza.

### Deployment con provisioning in modalità Over the Air OTA e altro ancora...

## Patch management e gestione delle vulnerabilità e dei sistemi

### Patch management

L'avanzata funzionalità di scansione delle vulnerabilità è completata dalla distribuzione automatica delle patch.

### Deployment rapida del software e del sistema operativo

Creazione, memorizzazione e deployment delle immagini del sistema da una console centralizzata. Questa è la soluzione ideale per effettuare l'upgrade a Microsoft Windows 10 o per il deployment di 150 applicazioni popolari identificate da Kaspersky Security Network.

### Gestione di hardware, software e licenze

I report dell'inventario software e hardware aiutano a controllare gli obblighi relativi alla licenza del software. Grazie alla gestione centralizzata del licensing si determina un risparmio sui costi.

# Assistenza e Professional Services

È disponibile assistenza qualificata in oltre 200 Paesi, da 34 uffici in tutto il mondo, 24 ore al giorno, 7 giorni la settimana, per 365 giorni all'anno. Approfittate dei pacchetti Premium (MSA) oppure contattate i nostri Professional Services per trarre il massimo vantaggio e ottimizzare il ROI dall'installazione delle soluzioni Kaspersky Lab.

## Provate voi stessi

Scoprite la True Cybersecurity. Visitate questa [pagina per provare la versione completa](#) di Kaspersky Endpoint Security for Business.

