

# Kaspersky Endpoint Detection and Response Optimum

Construiește o adevărată apărare complexă cu ajutorul răspunsului automatizat instant și cu analiza simplă a cauzelor principale

91% din toate organizațiile au fost afectate de atacuri cibernetice pe parcursul anului 2019, una din 10 organizații fiind ținta unui atac<sup>1</sup>.

## Problema

### Amenințările complexe aduc perturbare

Zilele malware-ului simplist s-au dus, iar amenințările au devenit din ce în ce mai complicate, aducând și mai multe întreruperi și pierderi și mai mari afacerilor, rămânând nedetectate și mai mult timp.

### Ești atacat

Aceste amenințări complexe au devenit mult mai ieftine și mai frecvente, așadar, organizațiile care credeau că sunt ferite trebuie acum să se acopere mai bine.

### Eficiența este imperativă

Lipsa de resurse cu care se confruntă organizațiile este ceea ce înrăutățește situația și mai mult. Cele mai valoroase două resurse sunt angajații iscusiți și timpul.

«O soluție EPP slabă va anula valoarea unui instrument EDR»<sup>2</sup>

«Oamenii și timpul devin astfel metoda de măsurare a randamentului investiției într-un instrument EDR»

## Cum putem ajuta

Kaspersky Endpoint Detection and Response (EDR) Optimum te ajută să rămâi în siguranță împotriva amenințărilor complexe și avansate oferind detecție avansată, un proces de investigare simplificat și o capacitate de răspuns automatizat.

### Abilități mai mult decât esențiale

Oferă o vizibilitate detaliată, instrumente de investigare simple și opțiuni de răspuns automatizate, atât pentru a detecta amenințarea, cât și pentru a dezvălui întreaga sa anvergură și origine. Astfel, se poate răspunde instant și preveni perturbarea afacerii.

### Adevărata apărare în profunzime

Reunește un set de instrumente de răspuns și detecție extrem de automatizată, ușor de folosit, cu protecție fără egal pentru endpointuri și cu detecția avansată a Kaspersky Endpoint Security for Business, pentru a crea o singură soluție unificată.

### Instrumentul inteligent care asigură eficiența

Îți economisește timpul și îți optimizează resursele umane și costurile cu IT-ul prin oferirea de instrumente de control centralizate simple și un nivel ridicat de automatizare. Un flux de lucru simplificat controlat dintr-o singură consolă disponibilă atât local, cât și în cloud<sup>3</sup>.

### Beneficii cheie

- Protejează-te împotriva amenințărilor perturbatoare, avansate și complexe care apar din ce în ce mai frecvent
- Fă economie de timp și resurse cu un instrument simplu și automatizat
- Vezi întreaga anvergură a amenințărilor complexe din toată rețeaua
- Înțelege cauza principală a amenințării și cum s-a ivit
- Evită pagubele suplimentare cu ajutorul răspunsului automatizat rapid

## Moduri esențiale de utilizare a EDR

### Răspunde la aceste întrebări importante

- Care sunt circumstanțele alertei?
- Ce măsuri s-au luat deja împotriva alertei?
- Amenințarea detectată este încă activă?
- Sunt și alte gazde atacate?
- Ce cale a urmat atacul?
- Care este adevărata cauză principală a amenințării?

### Descoperă întreaga anvergură a amenințării

Odată ce descoperi că ești în pericol din pricina unei amenințări globale – de exemplu, autoritatea de reglementare îți cere să efectuezi o scanare după un anume indicator de compromitere (IoC) – tu poți să:

- Importați IoC-uri din surse de încredere și poți efectua scanări periodice pentru a detecta semne ale unui atac
- Poți investiga în detaliu o alertă, genera IoC-uri bazate pe amenințările descoperite și efectua scanări ale întregii rețele pentru a afla dacă au fost afectate și alte gazde

### Poți adresa instant amenințările care se înmulțesc ușor

- Poți carantina în mod automat fișierele asociate cu amenințări complexe din toate endpointurile
- Poți izola în mod automat gazdele infectate atunci când găsești un IoC asociat unei amenințări care se răspândește rapid
- Poți preveni rularea fișierului rău intenționat și răspândirea acestuia prin rețea în timp ce efectuezi investigația

<sup>1</sup>Raportul global al riscurilor din domeniul IT realizat de Kaspersky, Kaspersky, 2019

<sup>2</sup>IDC, Endpoint Security 2020: Renașterea EPP și extinderea justificată și inevitabilă a EDR, Doc # US45794219, 2020

<sup>3</sup>Unele funcții și funcționalități nu pot fi gestionate cu ajutorul consolei din cloud. Pentru informații detaliate, vizitează

<https://kas.pr/epp-management-options>

# Acum poți:

## Vezi întreaga anvergură a amenințării

Vezi alertele de securitate din endpointurile tale și analizează-le mai departe, pentru a înțelege întreaga răspândire în lung și în lat a amenințării. Prin asta te asiguri că incidentele sunt neutralizate complet, fără nicio rămășiță a amenințării rămasă pe endpoint.

## Simplifică-ți fluxul de lucru

Fluxul de lucru simplificat printr-o singură consolă disponibilă atât la fața locului, cât și în cloud, este combinat cu scenariile și instrumentele de control simple ale EDR – acestea fiind: vizualizarea în detaliu, scanarea loC-urilor și opțiuni de răspuns care nu necesită foarte multe cunoștințe în domeniul securității cibernetice sau mult timp.

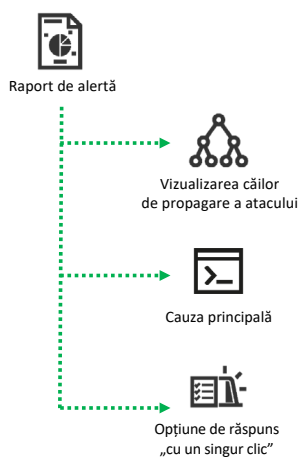
## Sporește-ți securitatea

Adăugarea suplimentară a Kaspersky Sandbox creează o soluție completă și integrată de securizare a endpointurilor, care oferă o apărare multistrat simplă, eficientă și foarte automatizată împotriva amenințărilor comercializate, complexe și evazive.

## Analizează informații detaliate despre alertă

Kaspersky EDR Optimum detaliază incidentele cu informațiile necesare și te ajută să faci legăturile dintre diferite evenimente prin vizualizarea căilor de propagare a atacului.

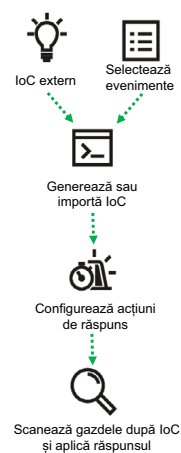
Este oferită vizibilitatea tuturor gazdelor din rețea prin scanarea indicatorilor de compromitere (loC-uri) fie importați, fie generați.



## Răspunde în mod automat

Configurează răspunsuri automatizate pentru amenințările din toate endpointurile, descoperite prin intermediul scanărilor loC sau răspunde la incidente imediat cum sunt depistate „cu un singur clic”.

Următoarele sunt posibile opțiuni de răspuns: izolarea gazdei, carantinarea fișierului, pornirea scanării gazdei și prevenirea execuției fișierului.



# Soluții EDR adiționale

Kaspersky Endpoint Detection and Response Optimum este una dintre soluțiile EDR pe care le oferim, fiecare din ele fiind create special să adreseze anumite nevoi ale clienților. S-ar putea să te intereseze:

## Kaspersky Endpoint Detection and Response

Soluție expertă EDR aclamată de industrie și de clienții săi, perfectă pentru organizațiile din domeniul IT care dețin echipe de specialiști iscusiți în securitatea IT. Soluția ajută la rezolvarea celor mai sofisticate și avansate atacuri ațintite asupra organizațiilor. Oferă abilități îmbunătățite de descoperire a amenințărilor, abilități eficiente de investigare, detectarea proactivă a amenințărilor și răspunsuri centralizate la incidente.

<https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr>

## Kaspersky Managed Detection and Response

Un serviciu care oferă non-stop detectare, prioritizare, investigare și răspuns, toate gestionate împreună și ajustate individual după nevoie. Acesta se bazează pe mai mult de 20 de ani de cercetări incredibile în domeniul amenințărilor. Serviciul îți oferă toate beneficiile majore de a avea propriul centru operațional de securitate, fără să trebuiască să înființezi un astfel de centru.

<https://www.kaspersky.com/enterprise-security/managed-detection-and-response>

Pentru a afla mai multe despre cum soluționează amenințările cibernetice Kaspersky Endpoint Detection and Response Optimum și, în același timp, simplifică munca echipei tale de securitate și consumă puține resurse, vizitează <http://www.kaspersky.com/enterprise-security/edr-security-software-solution>

Știri privind amenințările cibernetice: [www.securelist.com](http://www.securelist.com)  
Știri privind securitatea IT: [business.kaspersky.com](http://business.kaspersky.com)  
Securitate IT pentru întreprinderi:  
[kaspersky.com/enterprise](http://kaspersky.com/enterprise)  
Portalul cu informații privind amenințările:  
[opentip.kaspersky.com](http://opentip.kaspersky.com)

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

© 2020 AO Kaspersky Lab. Mărcile comerciale înregistrate și mărcile de servicii sunt proprietatea deținătorilor respectivi.



Ne-am dovedit valoarea. Suntem independenți. Suntem transparent. Ne-am luat angajamentul pentru crearea unei lumi mai sigure, în care tehnologia ne îmbunătățește viața. Tocmai de aceea o securizăm, pentru ca toată lumea să beneficieze de oportunitățile nelimitate pe care le oferă. Bazează-te pe securitatea cibernetică pentru un viitor mai sigur.



Proven.  
Transparent.  
Independent.