kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Vybudujte skutečně dokonalou obranu pomocí okamžitých automatických reakcí a jednoduché analýzy hlavních příčin

Problém

91 % všech organizací se v roce 2019 potýkalo s kybernetickými útoky a **1 z 10** organizací se stala obětí cíleného útoku.[1]

Složité hrozby způsobují narušení činnosti

Doba, kdy malware býval jednoduchý, je dávno pryč. Současné a mnohem komplikovanější hrozby způsobují firmám mnohem větší škody a ztráty a dokážou se dlouho skrývat bez povšimnutí.

Někdo na vás útočí

Komplexní hrozby jsou dnes levnější a častější, takže organizace, které si myslely, že jsou před nimi z obliga, se nyní před nimi musí mít na pozoru.

Na efektivitě záleží

Nedostatek lidských zdrojů, jemuž dnes organizace čelí, jen přilévá olej do ohně. Organizace nemají především čas řešit incidenty a zároveň k tomu ani nemají zkušené pracovníky.

Jak můžeme pomoci

„Nedostatečné EPP řešení znehodnotí účinnost EDR nástroje“[2]

„Lidé a čas se tak stávají novou metrikou návratnosti investice do EDR nástroje“[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum vás chrání před složitými a sofistikovanými hrozbami pomocí pokročilé detekce, zjednodušeného prošetřování a automatických reakcí.

Víc než jen základní funkce

Poskytuje podrobný přehled, jednoduché vyšetřovací nástroje a možnosti automatické reakce, abyste mohli nejen odhalovat hrozby, ale také zjišťovat jejich rozsah a původ a rychle na ně reagovat, než naruší fungování vaší firmy.

Skutečně dokonalá obrana

Nabízí intuitivní a vysoce automatizovanou sadu nástrojů pro detekci hrozeb a reagování na ně a dále bezkonkurenční ochranu koncových zařízení a pokročilé detekční funkce produktu Kaspersky Endpoint Security for Business v jednom řešení.

Inteligentní nástroj je zárukou efektivity

Ušetří vám čas a pomůže optimalizovat lidské zdroje a režijní náklady na IT pomocí jednoduchých centrálních ovládacích prvků a vysoké úrovně automatizace. Zjednodušený pracovní postup z jedné konzole, která je k dispozici místně i v cloudu.[3]

Klíčové výhody

- Chraňte se před čím dál častějšími a škodlivějšími pokročilými a složitými hrozbami
- Ušetřete čas a prostředky pomocí jednoduchého a automatického nástroje
- Mějte kompletní přehled o složitých hrozbách v celé síti
- Odhalujte hlavní příčiny hrozeb a jak k nim došlo
- Rychlými automatickými reakcemi předcházejte dalším škodám

Důležité možnosti uplatnění EDR

Odpovězte si na důležité otázky

- Jaký je kontext výstrahy?
- Které kroky jste už v souvislosti s výstrahou podnikli?
- Je zjištěná hrozba stále aktivní?
- Jsou napadeni i jiní hostitelé?
- Přes co útok probíhá?
- Co je skutečnou hlavní příčinou hrozby?

Seznamte se s úplným rozsahem hrozby

Jakmile se dozvíte, že jste ohroženi globální hrozbou (například vás úřady vyzvou, abyste provedli test na přítomnost určitého indikátoru napadení (IoC)), můžete:

- Importovat IoC z důvěryhodných zdrojů a spouštět pravidelné testy na známky útoku
- Důkladně prošetřit výstrahu, vygenerovat IoC na základě odhalených hrozeb a spustit testy napříč celou sítí, jestli nebyli napadeni i jiní hostitelé

Okamžitě reagujte na rychle se měnící hrozby

- Automaticky umisťujte do karantény soubory související s komplexními hrozbami na všech koncových zařízeních
- Automaticky izolujte infikované hostitele, když se najde IoC související s rychle se šířící hrozbou
- Zabraňte škodlivému souboru ve spuštění a šíření po síti v průběhu šetření

[1] The Kaspersky Global IT Risk Report, Kaspersky, 2019

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, dok. č. US45794219, 2020

[3] Některé funkce jsou přes cloudovou konzoli k dispozici jen v omezené formě. Kompletní informace najdete na adrese https://kas.pr/epp-management-options.

Nyní můžete:

Seznamte se s úplným rozsahem hrozby

Prohlížejte bezpečnostní výstrahy na koncových zařízeních a podrobně je analyzujte, abyste se seznámili s úplným rozsahem a závažností hrozby. Díky tomu dokážete každý incident zcela vyřešit a na koncových zařízeních po hrozbách nic nezůstane.

Zjednodušte své pracovní postupy

Zjednodušený pracovní postup na jedné konzoli, která je k dispozici místně a v cloudu, společně s jednoduchými scénáři a ovládacími prvky EDR, jako je podrobná vizualizace, testování na přítomnost IoC nebo možnosti reakce, jež nevyžadují velké odborné znalosti o kyberbezpečnosti ani příliš mnoho času.

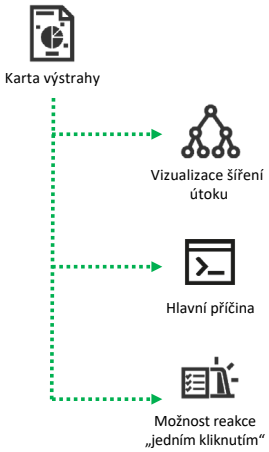
Posilte své obranné mechanismy

Dodatečně přidaný Kaspersky Sandbox vytváří úplné integrované řešení pro zabezpečení koncových zařízení, které poskytuje jednoduché, účinné a vysoce automatizované vícevrstvé obranné prvky proti obyčejným, složitým i sofistikovaným hrozbám.

Analyzujte obohacená data výstrah

Kaspersky EDR Optimum obohacuje incidenty o potřebné informace a pomáhá vám pochopit souvislosti mezi jednotlivými událostmi pomocí vizualizace šíření útoku.

Pomocí testů na přítomnost importovaných nebo vygenerovaných indikátorů napadení (IoC) získáte přehled napříč všemi hostiteli v síti.



Reagujte automaticky

Nastavte automatické reakce na hrozby zjištěné na kterémkoli koncovém zařízení na základě testů na přítomnost IoC nebo pomocí řešení „jedním kliknutím“ reagujte na incidenty hned po odhalení.

Možnosti reakce zahrnují izolaci hostitele, umístění souboru do karantény, spuštění testu hostitele nebo zablokování spuštění souboru.

Další možnosti uplatnění EDR

Kaspersky Endpoint Detection and Response Optimum je jedním z několika EDR řešení, jež nabízíme, přičemž každé z těchto řešení je přizpůsobené specifickým potřebám zákazníků. Také můžete zvážit:

Kaspersky Endpoint Detection and Response

Odborníky i zákazníky oceňované špičkové řešení EDR, které se hodí IT organizacím se zkušenými bezpečnostními týmy a které pomáhá důkladně analyzovat nejsofistikovanější pokročilé a cílené útoky. Nabízí funkce pro rozšířené odhalování hrozeb, účinné prošetřování incidentů, proaktivní lov na hrozby a centrální reakce na incidenty.
https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Plně spravované nástroje na míru, které umožňují nepřetržitou detekci, prioritizaci, prošetřování a řešení incidentů a které vycházejí z více než dvacetiletého špičkového výzkumu hrozeb, vám poskytují všechny hlavní výhody vlastního bezpečnostního centra bez nutnosti takové centrum zakládat.
https://www.kaspersky.com/enterprise-security/managed-detection-and-response

Další informace o tom, jak Kaspersky Endpoint Detection and Response Optimum řeší kybernetické hrozby a zároveň usnadňuje práci vašemu bezpečnostnímu týmu a nezatěžuje vaše prostředky, najdete na adrese
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Novinky v oblasti kybernetických hrozeb: www.securelist.com
Novinky v oblasti zabezpečení IT: business.kaspersky.com
Zabezpečení IT pro firmy: kaspersky.com/enterprise
Informační portál o hrozbách: opentip.kaspersky.com

www.kaspersky.com

Jsme prověření. Jsme nezávislí. Jsme transparentní. Zavázali jsme se k budování bezpečnějšího světa, ve kterém technologie zlepšují naše životy. Proto je zabezpečujeme, aby všichni lidé všude na světě mohli využívat nekonečné možnosti, které přinášejí. Zajistěte si počítačovou bezpečnost pro bezpečnější budoucnost.

Proven. Transparent. Independent.