IBM REAQTA NGAV+

IBM REAQTA-EON

Zesílená obrana proti všem hrozbám

ODSTRANÍ MEZERU V ANTIVIROVÉ BEZPEČNOSTI

Kybernetických útoků v posledních letech přibylo a jsou stále sofistikovanější. Jejich odhalování a náprava škod je zároveň pro bezpečnostní analytiky stále komplexnější.

Bez schopností nové generace, které by zlepšily prevenci a detekci útoků, je tradiční software, například antivirové nástroje, v podstatě neúčinný a nespolehlivý. Zatímco čtete tento text, u celé řady organizací, které nemají nezbytný bezpečnostní software nové generace, dochází k narušení činnosti v důsledku útoku, což je stojí peníze.

Systém IBM ReaQta-EON byl navržen s použitím nejmodernějších průlomových technologií v oblasti umělé inteligence a strojového učení. Poskytuje tedy klíčové bezpečnostní funkce, které každá organizace potřebuje, aby se dokázala ubránit moderním hrozbám. Vaše organizace nyní může bez námahy zlepšit svoji provozní odolnost a posílit obranu před rušivými kybernetickými útoky.

REAQTA
an IBM Company

PROČ SI BEZPEČNOSTNÍ TÝMY VYBÍRAJÍ IBM REAQTA-EON

Jednoduché použití, elegantní instalace. Antivirové řešení nové generace od firmy ReaQta ztělesňuje myšlenku „nepřetržité“ obrany za všech okolností, dokonce i v případě, že týmy pracují vzdáleně nebo off-line.

„Díky schopnosti odhalit útočníka ještě předtím, než do systému pronikne, může IBM ReaQta zajistit odolnost proti náhlému průniku.“

Frost & Sullivan

Systém, kterému důvěřují analytici po celém světě. Nedílná součást projektu „Multisandbox“.

VirusTotal

„Brilantní ochrana koncových bodů, jejíž komplexní a snadno použitelné uživatelské rozhraní umožňuje problém snadno izolovat a vyřešit.“

Telco Provider

„Nyní máme lepší přehled o našich koncových bodech a dokážeme odhalit hrozby, které antivirový software přehlédne. Bezpečnostní pozice naší organizace se výrazně zlepšila.“

Finanční instituce

NEPŘEKONATELNÁ OCHRANNÁ TECHNOLOGIE

IBM ReaQta-EON spojuje tradiční i moderní metody obrany s nejmodernějšími strategiemi umělé inteligence a strojového učení. Útočníky tak dokáže zastavit v reálném čase. Takový systém vás ochrání před známými i neznámými hrozbami, takže omezí nutnost uchylovat se k nákladným reakcím a odstraňováním škod.

RYCHLÁ A SNADNÁ SPRÁVA

Díky autonomnímu ochrannému modulu IBM ReaQta-EON a optimalizovanému uživatelskému rozhraní si analytici vystačí jen s minimální správou a mohou snadno reagovat na hrozby. Cloudový hlavní panel je přístupný prostřednictvím jakéhokoli webového prohlížeče, a to kdykoli a z libovolného místa. Lze ho tedy snadno spravovat, kdykoli je zrovna potřeba.

CLOUDOVÉ ANTIVIROVÉ ŘEŠENÍ NOVÉ GENERACE+

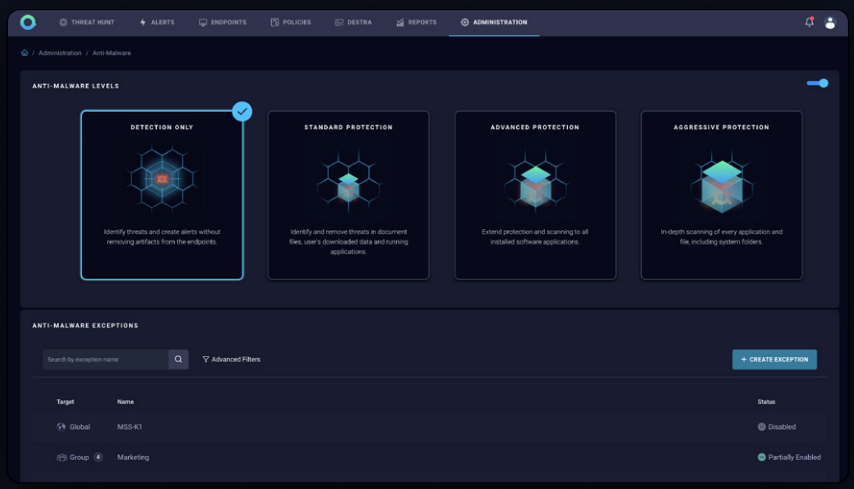
Moduly EON jsou cloudové a do plného provozu je uvedete během několika sekund. Pro uživatele to znamená rychlou instalaci s velkou finanční úsporou. Týmy ušetří značné náklady na infrastrukturu a údržbu, protože server a software Hive Brain™ za uživatele zajistí a spravuje společnost IBM ReaQta.

Poznámka: Instalaci lze provést snadno pomocí skupinových zásad (GPO), správce konfigurací systémového centra (SCCM) nebo ručně.

ŠKÁLOVATELNÉ ZABEZPEČENÍ

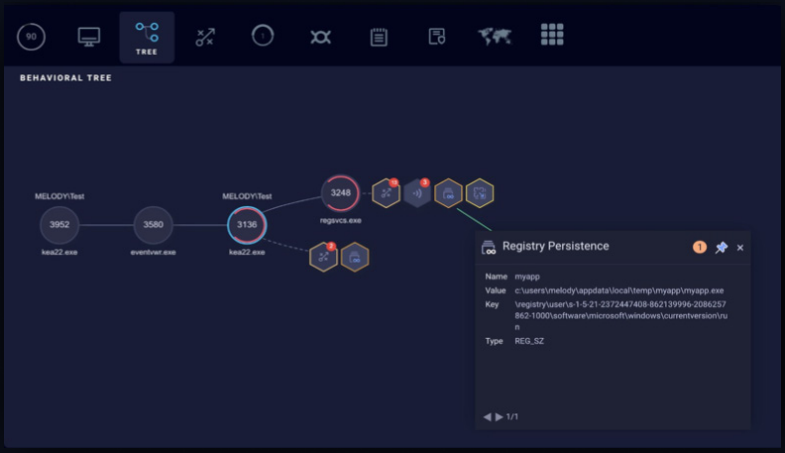
Díky IBM ReaQta vaše ochrana roste spolu s vaším byznysem. Kdykoli bude potřeba rozšířit zabezpečení, budete moci hladce přidat pokročilé funkce a analýzy, například vyhledávání hrozeb, cloudové sledování hrozeb, artefaktovou analýzu, automatizaci odstraňování následků, detekční strategie a přístup pomocí rozhraní API. Společnosti, které požadují neustálé sledování, mohou zvolit nepřetržité spravované služby, které bezpečnostní tým IBM ReaQta poskytuje prostřednictvím IBM ReaQta-MDR.

Čtyři snadno nastavitelné režimy boje s malwarem

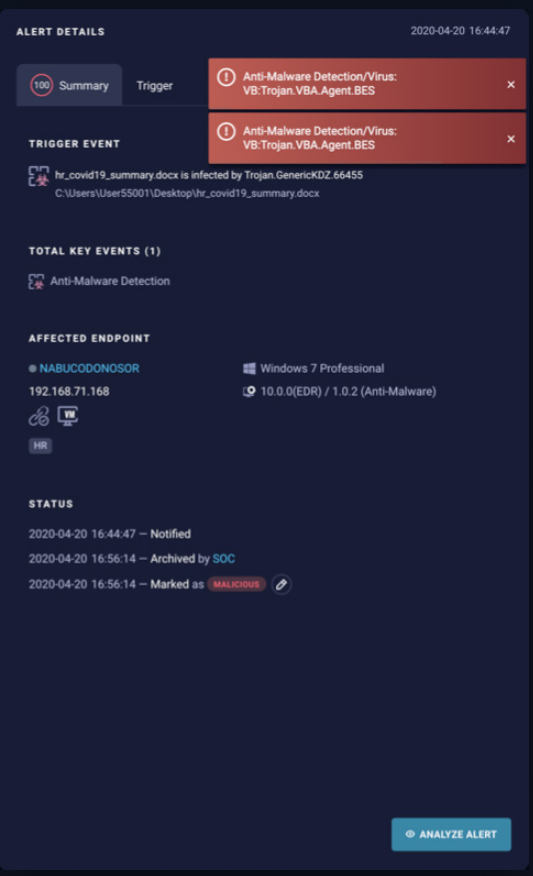


ČÍM IBM REAQTA-EON VYNIKÁ?

IBM ReaQta-EON spojuje osvědčené technologie s vysoce pokročilými metodami detekce, kontroly před spuštěním a prevence, a chrání tak klíčová data vaší organizace a její životně důležité informace.



Strom chování ReaQta poskytuje komplexní upozornění a přehled o útoku



Upozorňování a prevence v reálném čase

Hlavní funkce	Jak je IBM ReaQta-EON zajišťuje
PREVENCE PŘED SPUŠTĚNÍM	Pomocí dynamické emulace a technologie sekvencování útoků detekuje škodlivý kód v souborech ještě před jejich spuštěním. Zdrojový kód souboru je před jeho úplným spuštěním během několika milisekund několikrát zkontrolován, takže je v podstatě zabráněno spuštění potenciálně škodlivých souborů.
NANO OS ™ A DUÁLNÍ UMĚLÁ INTELIGENCE	Každý modul koncového bodu obsahuje technologii duální umělé inteligence a Nano OS™ od firmy IBM ReaQta. Je tedy schopen rozšířené proprietární detekce a autonomního provozu i v případě, jsou zařízení off-line. Naše technologie umělé inteligence detekuje pokročilé a nově vzniklé hrozby díky hlubokému porozumění infrastruktuře a určení jejího standardního chování.
ÚPLNÝ PŘEHLED O ÚTOCÍCH	Díky umělé inteligenci IBM ReaQta dokážete získat a korelovat všechny informace z komplexních upozornění, takže z nich v reálném čase vznikne vyčerpávající přehled situace. A není k tomu potřeba žádný manuální zásah.
KARANTÉNA MALWARU	IBM ReaQta-EON zajišťuje karanténu nežádoucího malwaru, aby jej bylo možno dále prověřit a odstranit. V tom se liší od klasické ochrany, která takové soubory včetně falešných poplachů automaticky maže.
OCHRANA PŘED RANSOMWAREM	IBM ReaQta-EON pomocí analýzy chování rozšiřuje ochranné schopnosti i na obranu před nově vzniklými hrozbami a útoky ransomwaru. Analýzou chování souborů podle sekvence kybernetických útoků dokáže IBM ReaQta-EON odhalit hrozící útok a zastavit škodlivé procesy ještě před jejich provedením.
SIGNATURY A HEURISTICKÁ KONTROLA	Účelem této funkce je průběžně zastavovat známé útočníky prostřednictvím osvědčených bezpečnostních technik heuristiky a prevence založené na signaturách.

VYZKOUŠET ZDARMA

PODPOROVANÉ ARCHITEKTURY

Společnost IBM ReaQta

Naše společnost vznikla spojením někdejších expertů na ofenzivní kybernetickou bezpečnost se zkušenostmi ze zpravodajských služeb a odborníky na pátrání po hrozbách. Společné zkušenosti obránců a útočníků pomohly nalézt nový způsob, jak překonat omezení, která tradiční bezpečnostní nástroje představují. IBM ReaQta řeší zabezpečení koncových bodů novým způsobem. Na zařízení pohlíží jako na entity s dynamickým a vyvíjejícím se chováním. Tento přístup, spolu se špičkovou umělou inteligencí, zaručuje organizacím všech velikostí nepřekonatelný přehled a rozsáhlé možnosti vyhledávání a sledování hrozeb.

NAVŠTIVTE FREEDIVISION.COM

FREEDIVISION
for safety reasons