IBM REAQTA HIVE

IBM ReaQta MDR

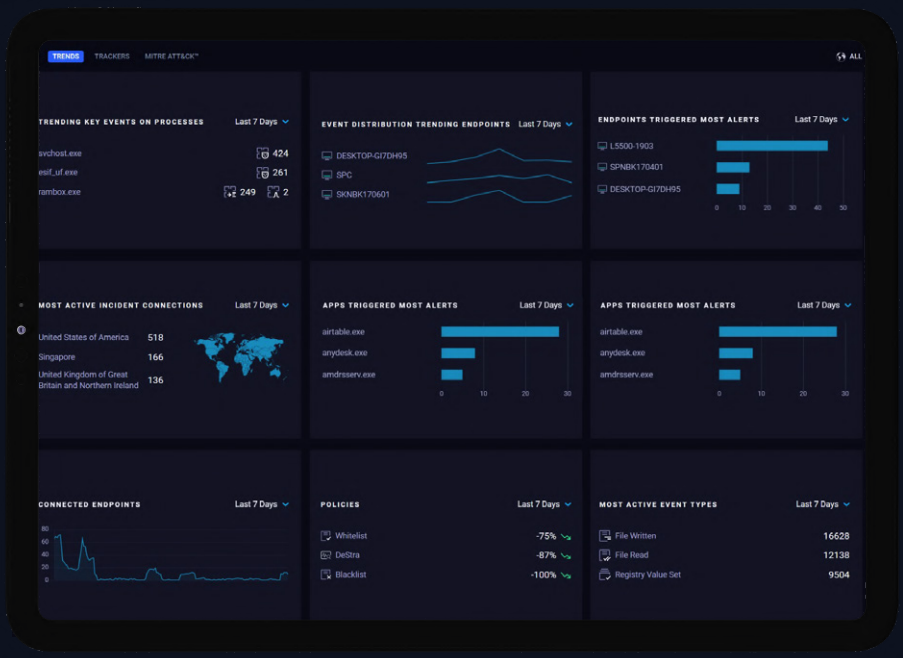
Zaručená bezpečnost 24×7×365

REAQTA
an IBM Company

NAVŠTIVTE FREEDIVISION.COM

ZABEZPEČTE KONTINUITU A RŮST PODNIKÁNÍ

Digitalizace a přechod do cloudu mění způsob, jakým organizace fungují. Lepší konektivita a větší škálovatelnost ale zároveň zvětšují kybernetická rizika. Najít vhodnou rovnováhu mezi bezpečností a škálováním je náročný úkol, v němž zabezpečení často selhává. Pro firmu to mívá dalekosáhlé a potenciálně vážné důsledky. Služby IBM ReaQta MDR organizacím pomáhají zaměřit se na růst, zatímco se tým expertů stará o hlavní aspekty jejich kybernetické bezpečnosti.



JAK SLUŽBA IBM REAQTA-MDR ZAJIŠŤUJE BEZPEČNOST ORGANIZACÍ

IBM REAQTA MDR

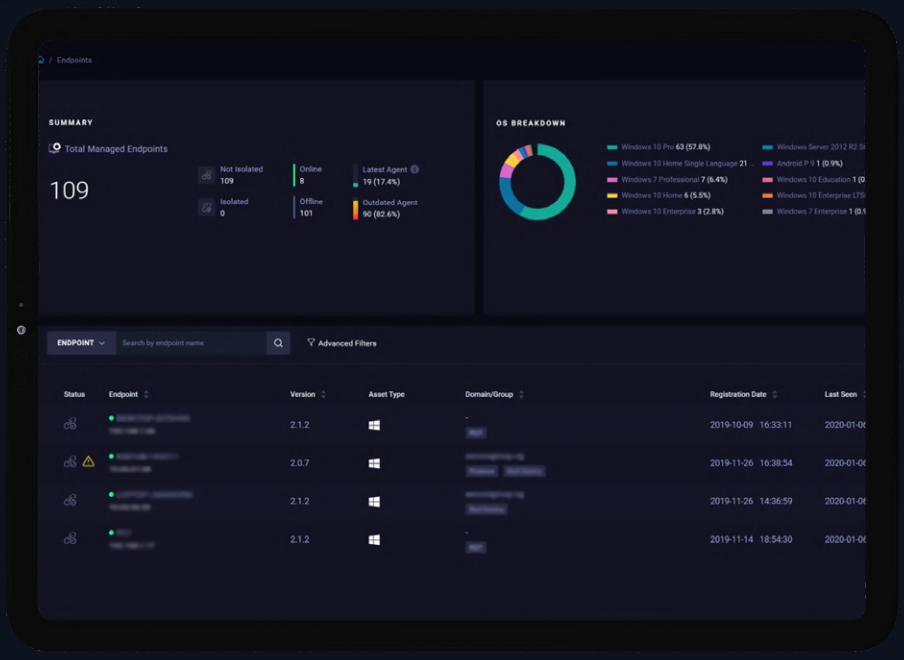
Tým expertů, který má rozsáhlé zkušenostmi s řešením závažných útoků, zajišťuje průběžnou detekci hrozeb a v reálném čase řeší incidenty na serverech a koncových bodech (notebooky, mobilní zařízení). Analytický tým IBM ReaQta-MDR pracuje jako prodloužená ruka organizací, které sice mají jen malý tým IT, ale potřebují nepřetržitě sledovat kybernetické hrozby a omezovat jejich následky.

Hlavní problémy	Jak vám může pomoci ReaQta-MDR
• Omezený přehled o infrastruktuře	• Úplný přehled o aktivitách koncových bodů umožňující odhalování hrozeb a anomálií v reálném čase.
• Nedostatek pracovníků kybernetické bezpečnosti	• Bezpečnostní analytici IBM ReaQta-MDR zajišťují nepřetržité bezpečnostní monitorování a aktivní vyhledávání hrozeb včetně nových i aktivních.
• Malé schopnosti v oblasti reakce a nápravy	• Omezení škod způsobených výpadky činnosti díky rychlé reakci, nápravě a odstraňování následků týmem IBM ReaQta, který se specializuje na bezpečnostní incidenty.
• Omezené možnosti posouzení situace a tvorby zpráv	• Tým IBM ReaQta-MDR během pouhých pár hodin po útoku vypracuje technickou zprávu i zprávu pro management, které našim zákazníkům pomohou posoudit místo a příčiny potenciálního narušení bezpečnosti a informovat o nich.

PODPOROVANÉ ARCHITEKTURY

SLUŽBY IBM REAQTA MDR

Zajistěte kontinuitu podnikání



Odolnost vůči útokům

Pomocí unikátního NanoOS mohou bezpečnostní analytici získávat podrobná data z koncových bodů a zároveň chránit sledovací platformu před útoky, které by se ji pokoušely vyřadit. Kompletní mapování událostí MITRE ATT&CK – přímo na hlavní panel ReaQta – a systém s dvojí umělou inteligencí zajišťují rychlou automatickou detekci a sledování veškerých zlovolných aktivit.

Menší náklady

Platforma IBM ReaQta-Hive, kterou IBM ReaQta-MDR používá, pracuje automaticky a na bázi umělé inteligence. Proto umožňuje v reálném čase odhalovat hrozby a omezovat dobu, po kterou mohou útočníci působit škody.
Analytici díky ní mohou okamžitě reagovat na jakoukoli hrozbu. Nápravné činnosti jsou prováděny přímo analytickým týmem, aniž by to narušilo kontinuitu činnosti firmy.

Jednoduchost

Naše platforma zajišťuje úplný přehled o infrastruktuře organizace.
To umožňuje podrobná vyhledávání a sledování hrozeb na bázi ukazatelů chování a příznaků napadení, takže lze odhalovat a řešit aktivní útoky, spící hrozby, laterální přesuny a útoky vedené skrz dodavatelský řetězec.

Nepřetržitá obrana

Analytici IBM ReaQta-MDR zajišťují nepřetržité sledování kybernetické bezpečnosti 365 dní v roce, 7 dní v týdnů a 24 hodin denně. Odhalují narušení bezpečnosti, analyzují rozsah škod a na každou nalezenou hrozbu příslušným způsobem reagují.

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.