kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Pokročilá detekce a ochrana před neznámými a skrytými hrozbami bez nutnosti najímat odborníky na bezpečnost IT.

Současné pokročilé kyberútoky mohou paralyzovat celé společnosti nebo způsobit ekonomický otřes či ztrátu reputace. Ztráta finančních prostředků, obchodního tajemství nebo důvěry zákazníků v důsledku selhání poskytování služeb a podobných negativních dopadů spojených s útokem mohou mít vážný dopad na stabilitu a prosperitu společnosti. K ochraně před rychle se rozvíjejícími kyberútoky nejsou tradiční nástroje určené k ochraně perimetru sítě (firewall, e-mailové a internetové brány nebo proxy servery) nebo pracovních stanic a serverů (antivirová ochrana a základní ochrana na úrovni komplexní platformy pro ochranu koncových bodů) zdaleka dostačující. Z toho důvodu moderně smýšlející společnosti musí pečlivě zvážit použití specializovaných nástrojů na detekci, vyšetřování komplexních hrozeb a náležité reakce na ně.

Řešení Kaspersky Sandbox je vhodné pro:

- Organizace bez specializovaného týmu pro bezpečnost IT, kde se touto problematikou zaobírá oddělení IT.
- Malé podniky, které nechtějí na bezpečnost IT vynaložit další náklady.
- Velké organizace, jejichž infrastruktura se nachází na různých místech a nemají lokálně řešeného odborníka na bezpečnost IT.
- Organizace, které potřebují zajistit, že jejich analytik bezpečnosti IT má čas věnovat se důležitější náplni práce.

Již přes dvacet let společnost Kaspersky vytváří zabezpečovací nástroje pro organizace různých velikostí, odborností a úrovně zabezpečení IT. Díky dlouhodobému výzkumu a vývoji, který přinesl pokrok ve vyhledávání a šetření hrozeb a náležité reakci na ně, zůstává společnost Kaspersky v čele boje s kyberzločinem.

Do širokého spektra produktů a služeb pro boj s komplexními hrozbami společnosti Kaspersky se řadí:

- Špičkové řešení Kaspersky Anti Targeted Attack Platform, které slouží k detekci a vyšetřování komplexních hrozeb a cílených útoků na úrovni sítě.
- Řešení Kaspersky Endpoint Detection and Response, které slouží k detekci, vyšetřování komplexních hrozeb a náležité reakci na ně na úrovni pracovních stanic a serverů.
- Řešení Kaspersky Threat Intelligence Portal, které poskytuje přístup k nástroji Cloud Sandbox, analytickým zprávám o pokročilých perzistentních hrozbách (APT) a dalším službám.

K naplnění plného potenciálu těchto řešení a služeb je ovšem potřeba, aby společnosti měly dostatečně vzdělané a zkušené plnohodnotné oddělení pro bezpečnost IT. Právě celosvětový nedostatek odborníků v oblasti boje proti komplexním hrozbám a jejich finanční náročnost je nezřídka klíčovou překážkou v obstarání takovýchto druhů řešení a služeb.

Řešení Kaspersky Sandbox, které je založené na patentované technologii (pod číslem patentu US 10339301B2) pomáhá organizacím čelit rostoucímu počtu vysoce komplexních moderních hrozeb, které uniknou současně dostupné ochraně koncových bodů. Řešení Kaspersky Sandbox doplňuje dosah řešení Kaspersky Endpoint Security for Business a významně navyšuje úroveň zabezpečení pracovních stanic a serverů před zatím neznámým malwarem, nejnovějšími viry a ransomwarem, zneužitím nultého dne a dalších hrozeb – bez potřeby vysoce kvalifikovaného analytika informační bezpečnosti.

Díky tomu nemusí malé podniky vynaložit prostředky na najímání takovýchto odborníků. Velkým podnikům s distribuovanými sítěmi toto řešení zase umožňuje optimalizovat náklady vynaložené na účinnou ochranu vzdálených pracovišť a snížení pracovní zátěže jejich analytiků informační bezpečnosti.

Možnosti nasazení:
Řešení Kaspersky Sandbox je možno získat v podobě ISO obrazu s předkonfigurovaným systémem CentOS 7 a dalšími potřebnými komponentami. Lze jej nasadit na fyzické či virtuální servery založené na VMware ESXi.

Integrace:
- Systémy SIEM mohou z nástroje Kaspersky Sandbox přijímat informace o detekcích. Tato data se odesílají přes Kaspersky Security Center v toku ostatních událostí.
- V nástroji Kaspersky Sandbox je zahrnuto také rozhraní API, pro integraci s dalšími řešeními, díky čemuž lze soubory odesílat do nástroje Kaspersky Sandbox ke kontrole a lze vyžádat verdikt o bezpečnosti souboru.

Škálovatelnost
Naše řešení je jednoduše škálovatelné, podporuje konfigurace od 250 až do 5 000 ochráněných koncových bodů a dokáže zajišťovat nepřetržitou ochranu rozsáhlých infrastruktur.

Clustering
Několik serverů je možné shlukovat za účelem větší kapacity a vysoké dostupnosti.

Jak to funguje

Řešení Kaspersky Sandbox využívá našich nejlepších odborných praktik v boji s komplexními hrozbami a útoky na úrovni pokročilých perzistentních hrozeb a je plně integrováno s řešením Kaspersky Endpoint Security for Business. Tyto funkce lze spravovat přes naši sjednocenou konzoli Kaspersky Security Center.

Agent Kaspersky Endpoint Security for Business vyžádá data o podezřelých objektech ze sdílené operační mezipaměti verdiktů, která se nachází na serveru Kaspersky Sandbox. Pokud databáze tento soubor již zná, nástroj Kaspersky Endpoint Security for Business obdrží verdikt a provede jedno nebo více z následujících nápravných opatření:

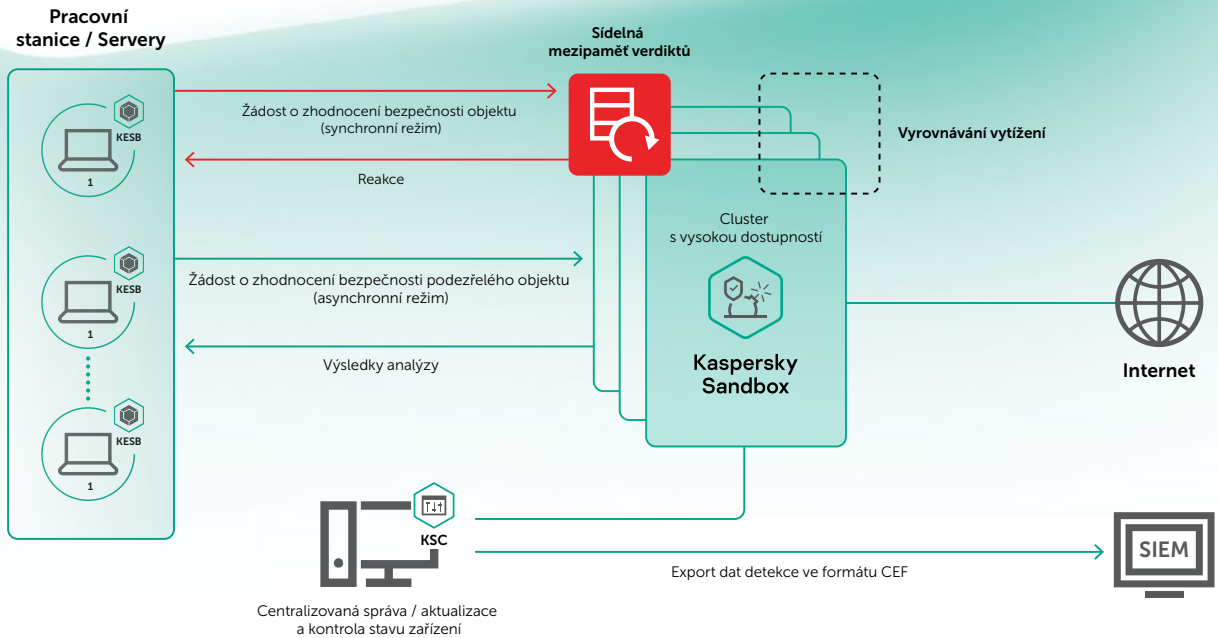
- Soubor odstraní a přesune jej do karantény
- Upozorní uživatele
- Zahájí kontrolu kritických oblastí
- Vyhledá zjištěný objekt na dalších zařízeních ve spravované síti.

Pokud není možné z databáze obdržet verdikt o příslušném objektu, nástroj Kaspersky Endpoint Security for Business pošle podezřelý soubor do izolovaného prostředí (sandbox) a počká na odpověď. Sandbox obdrží žádost na skenování souboru, které proběhne v prostředí izolovaném od skutečné infrastruktury.

Ke skenování souborů dochází na virtuálních strojích vybavených nástroji, které emulují typické pracovní prostředí (operačním systémem nebo nainstalovanými aplikacemi). Za účelem zhodnocení bezpečnosti souboru proběhne analýza chování, jsou nashromážděny a analyzovány artefakty, a pokud objekt provede škodlivé operace, nástroj Sandbox jej označí za malware. Výsledkem analýzy v sandboxu je verdikt, který se k souboru přiřadí.

Až se analýza souboru dokončí, verdikt se v reálném čase odešle do sdílené operační mezipaměti verdiktů, aby mohli jiní uživatelé s řešením Kaspersky Endpoint Security for Business rychle získat data o bezpečnosti skenovaného objektu, aniž by museli znovu tentýž soubor analyzovat. Popsaný postup umožňuje rychlé zpracování podezřelých objektů, snižuje vytížení serverů Kaspersky Sandbox a celkově zlepšuje rychlost a efektivnost reakce na hrozby.

Nástroj Kaspersky Sandbox je nezbytným rozšířením k řešení Kaspersky Endpoint Security for Business. Automaticky blokuje pokročilé, neznámé a komplexní hrozby bez nutnosti využívat další zdroje a zároveň umožní analytikům bezpečnosti věnovat se jiné pracovní náplni.



Novinky v oblasti kybernetických hrozeb: www.securelist.com
Novinky v oblasti zabezpečení IT: business.kaspersky.com
Zabezpečení IT pro malé až střední podniky: kaspersky.com/business
Zabezpečení IT pro firmy: kaspersky.com/enterprise

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.

Zjistěte více na stránce kaspersky.com/transparency

Proven. Transparent. Independent.