

Antimalwarové technologie

"Nastavení standardu ochrany, přesnosti a snadné integrace"

Finanční zisk je hnací silou exponenciálního růstu malwaru a jeho sofistikovanosti - každý den je objeveno více než 390 000 nových variant malwaru. Rychle se měnící technologie a heterogenní prostředí jen zhoršují zranitelnost, protože otevírají další slabé články, které se provozovatelé malwaru snaží využít.

Hrozby jsou navrženy tak, aby byly nenápadné, aby zůstaly neodhaleny tak dlouho, jak jen to bude možné. Záškodníci se snaží využívat všechny vektory, které mají k dispozici: exploity, víry, trojské koně, hackerské útoky, phishingové útoky, a v mnoha případech i jejich kombinace, aby byli co nejúčinnější a zůstali mimo pozornost. Tyto vícenásobné vektory útoků a persistentní hrozby zvyšují poptávku firem a organizací po řešeních vícevrstvé ochrany.

Bitdefender Antimalware SDK

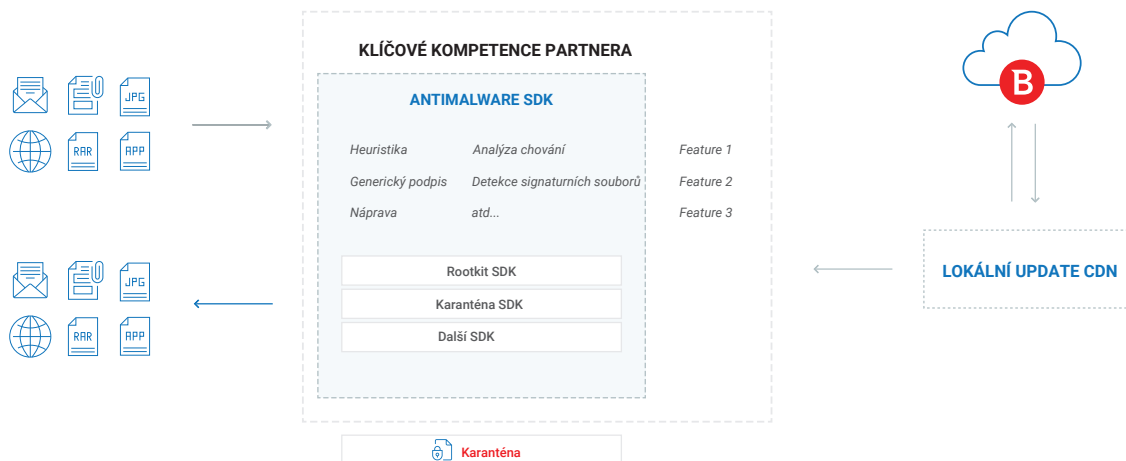
Bitdefender Antimalware SDK nabízí vícevrstvé, špičkové technologie ochrany, které lze integrovat do vašeho řešení jako přidanou hodnotu. Může pomoci odůvodnit navýšení ceny uceleného řešení stávajícím zákazníkům, kteří používají starší řešení, a může pomoci vytvořit nové obchodní příležitosti s využitím poptávky trhu po ochranných sadách.

Bitdefender Antimalware SDK lze snadno implementovat na koncových bodech, v síti, na perimetru, na bráně a na cloudových platformách. Sada Antimalware SDK může být doplněna širokou škálou bezpečnostních technologií Bitdefender, aby bylo možné posílit zabezpečení, chránit před dalšími vektory hrozeb, a reagovat na další poptávku trhu.

Různé technologie

Sada Antimalware SDK implementuje několik technologií a detekčních metod, aby zajistila špičkovou přesnost a výkon detekce známých i neznámých hrozeb, které využívají scénáře zero-day.

- Heuristická analýza: poskytuje proaktivní ochranu proti polymorfnímu malwaru; využívá emulaci procesů při přístupu k identifikaci neznámého malwaru; emulace procesů probíhá v simulovaném lokálním sandboxu.
- Behaviorální analýza: zajišťuje proaktivní detekci hrozeb typu zero-day na základě nepřetržitého monitorování procesů v reálném čase po celou dobu jejich trvání.
- Obecná detekce: odhalí všechny (včetně aktuálně neznámých) vzorky známé rodiny malwaru.
- Detekce založená na signaturách detekuje všechny známé vzorky malwaru.



Který antimalwarový SDK je vhodný pro vaše potřeby?

Výběr správného Antimalware SDK je rozhodující pro získání nejlepšího obchodního řešení pro danou situaci, ale také řešení, které nejlépe vyhovuje vašemu vývojovému týmu a architektuře.

	Endpoint	Gateway	Appliance	Android
Vysoká úroveň	Nejvhodnější	N/A	N/A	N/A
Jádro	Vhodné	Vhodné	Vhodné	N/A
Klientský server	N/A	Nejvhodnější	Nejvhodnější	N/A
Rychlé skenování	Nejvhodnější	N/A	N/A	N/A
Android Online/Offline	N/A	N/A	N/A	Nejvhodnější
Posílení ochrany	Nejvhodnější	Vhodné	Vhodné	N/A

Jádro Antimalware SDK

- Příklad použití: lze integrovat do koncových bodů, síťových zařízení, bran a cloudových služeb.
- Rozhraní: Umožňuje integraci prostřednictvím sdílené knihovny (Windows/Unix) nebo rozhraní COM (pouze Windows).
- Podpora: více platform (ARM, MIPS, X86, PowerPC) a operačních systémů (Windows, MAC a Linux) ze stejného rozhraní API; nativní podpora 32bitových a 64bitových platform.

Vysokourovňový antimalware SDK

- Příklad použití: obvykle se používá v řešeních zabezpečení koncových bodů
- Rozhraní: Umožňuje integraci prostřednictvím sdílené knihovny (Windows/Unix) nebo rozhraní COM (pouze Windows).
- Podpora: architektura x86/x86_64; více operačních systémů (Windows, MAC, Linux); nativní podpora 32bitové/64bitové platformy.

Antimalware SDK pro klienty a servery

- Příklad použití: provoz na bráně, firewall / UTM, web / e-mail
- Poskytuje: antimalware, sandbox, reputaci URL a antispamovou ochranu.
- Rozhraní: na úrovni protokolu i vazby na jazyk C\C++; umožňuje integraci prostřednictvím sdílené knihovny.
- Podporuje: ICAP a vestavěný textový protokol

Antimalware SDK for Android

- Příklad použití: Zařízení se systémem Android
- Rozhraní: Rozhraní API jazyka Java
- Podporuje: Operační systém Android 2.2 a vyšší; nativní podpora platformy ARM

Advanced Threat Control SDK

- Příklad použití: Koncové body systému Windows
- Poskytuje: ochranu před exploity typu zero-day a pokročilými trvalými hrozbami (APT)
- Rozhraní: Vazby na rozhraní C; umožňuje integraci prostřednictvím dynamicky propojené knihovny
- Podporuje: Windows OS 7 a vyšší

DLOUHODOBĚ VEDOUcí POZICE V NEZÁVISLÝCH TESTECH AV-COMPARATIVES



Kontaktujte nás

Další informace o řešeních Bitdefender získáte na adrese www.bitdefender.cz/firemni-reseni.

O licencování technologií společnosti Bitdefender.

Společnost Bitdefender poskytuje komplexní řešení kybernetické bezpečnosti a pokročilou ochranu před hrozbami více než 500 milionům uživatelů ve více než 150 zemích. Od roku 2001 společnost Bitdefender trvale vytváří oceňované bezpečnostní technologie pro podniky a spotřebitele, a stala se poskytovatelem, kterého si vybrali přední nezávislí dodavatelé softwaru (ISV), dodavatelé hardwaru, poskytovatelé služeb a podnikové organizace, které chtějí integrovat bezpečnostní technologie do svých produktů a služeb. V současné době má společnost Bitdefender více než 150 technologických partnerů po celém světě. Další informace jsou k dispozici na adrese www.bitdefender.cz/firemni-reseni

Bitdefender®

Založeno 2001, Romania
Počet zaměstnanců 1800+

Sídlo
Enterprise HQ – Santa Clara, CA, United States Technology HQ –
Bucharest, Romania

COUNTRY PARTNER pro Českou republiku a Slovensko
IS4 security s.r.o., Praha, Česká republika
tel.: +420 245 501 800
email: info@bitdef.cz