

Datový list

Avast Essential Business Security

Avast Essential Business Security pomáhá zabezpečit zařízení v malých firmách, které chtějí mít vzdálený přehled a centrálně řízenou ochranu před viry, phishingem, ransomwarem a pokročilými kybernetickými útoky.

Základní kybernetická ochrana a ovládání zabezpečení pro malou firmu

Ochrana zařízení

Zabezpečte svá firemní zařízení před kybernetickými útoky

Počítače a servery jsou hlavními vstupními body k firemním datům. Posilte zabezpečení svých zařízení před online i offline hrozbami, jako jsou malwarové infekce, následná zpomalení a zneužití. Dopřejte si více klidu díky antiviru nové generace od Avastu se šesti ochrannými štíty a sítí pro detekci hrozeb využívající umělou inteligenci.

Ochrana dat

Chraňte se před ransomwarem a úniky dat

Zvyšte zabezpečení své firmy a zákaznických dat před úniky, zašifrováním a výpadky pomocí firewallu a několika ochranných štítů.

Online zabezpečení a soukromí

Vyhňte se phishingu, slídilům, podvodům a dalším online hrozbám

Pomozte zaměstnancům udržet jejich online aktivity ve větším bezpečí a soukromí pomocí Ochrany webové kamery, Ochrany hesel a Ochrany před phishingem. Mohou tak zůstat produktivní a mít méně starostí, aniž by záleželo na tom, odkud pracují.

Vzdálená správa

Postarejte se o zabezpečení svých zařízení při rozšiřování a růstu

S růstem firmy rostou i potřeby v oblasti zabezpečení. S naší online platformou pro správu můžete ovládat svá zařízení, bezpečnostní služby Avastu a jejich předplatná z jednoho místa – kdykoli a odkudkoli.

Funkce

Ochrana zařízení



Souborový štít

Testuje programy a soubory uložené v počítači v reálném čase na přítomnost hrozeb ještě předtím, než umožní jejich otevření, spuštění, změnu nebo uložení. Souborový štít v případě nálezu malwaru zabrání příslušnému programu či souboru v infikování počítače.



Sandbox

Umožňuje vám prohlížet web nebo spouštět aplikace ve zcela izolovaném a bezpečném prostředí. Vše, co v Sandboxu spustíte nebo zobrazíte, nebude moci vašemu počítači nijak uškodit. To se hodí, když chcete spouštět podezřelé nebo nedůvěryhodné aplikace bez obav, že by vás mohly ohrozit.



Webový štít

V reálném čase testuje data přenášená při procházení internetu, čímž pomáhá bránit malwaru, jako jsou škodlivé skripty, ve stažení a spuštění v počítači.



CyberCapture

Zjišťuje a analyzuje ojedinělé podezřelé soubory. Pokud se takový soubor pokusíte spustit, CyberCapture ho v počítači uzamkne a pošle do Virové laboratoře Avastu, kde bude analyzován v bezpečném virtuálním prostředí.



E-mailový štít

Testuje příchozí a odchozí e-mailové zprávy v reálném čase a hledá v nich škodlivý obsah, jako jsou viry. Testování se týká pouze zpráv odeslaných nebo přijatých pomocí desktopových e-mailových klientů, jako jsou Microsoft Outlook nebo Mozilla Thunderbird.



Celkový test

Hledá malware, zastaralé aplikace, nebezpečná nastavení a podezřelé doplňky.



Behaviorální štít

Sleduje všechny procesy v počítači a v reálném čase zjišťuje, zda se nechovají podezřele, což může být známkou toho, že obsahují nebezpečný kód. Je navržen tak, aby zjišťoval a blokoval podezřelé soubory na základě jejich podobnosti s jinými známými hrozbami, i když ještě nejsou přidány do databáze virových definic.



Záchranný disk

Umožňuje otestovat počítače před spuštěním systému. Výrazně se tím zvýší šance na nalezení a odstranění malwaru, neboť v takovém případě malware nedokáže účinně reagovat. Pokud máte podezření, že je počítač infikován malwarem, a žádné jiné antivirové testy nedokázaly problém vyřešit, můžete použít Záchranný disk.



Ochrana dat a síť



Pokročilý firewall

Monitoruje síťový provoz mezi zařízeními zaměstnanců a internetem. Vylepšeným blokováním nebezpečných nebo zbytečných datových přenosů zajistí lepší ochranu firmy před škodlivou manipulací s daty.



Štít proti ransomwaru

Posilí ochranu vašich citlivých dat a jiných důležitých firemních dokumentů před změnami, odstraněním nebo zašifrováním způsobeným útoky ransomwaru. Můžete určit, které aplikace smí přistupovat k vašim chráněným složkám, a ostatní přístupy zablokovat.



Štít vzdáleného přístupu

Pomáhá chránit před zneužitím protokolu RDP a útoky hrubou silou tím, že vám umožňuje zvolit, kdo smí na dálku přistupovat ke koncovým zařízením, a blokovat nevyžádaná připojení.



Inspektor sítě

Pomáhá zabezpečit síť před útočníky a zneužitím dat. Kontroluje stav sítě, zařízení připojená k síti a nastavení routeru. Rozpoznává tak potenciální bezpečnostní problémy, které by otevíraly vrátka různým hrozbám.



Skartovač dat

Umožňuje nevratně vymazat soubory nebo disky, aby nikdo nemohl obnovit a zneužít vaše data.



Ochrana serveru SharePoint

Kontroluje všechny soubory nahrané do sdíleného úložiště a pomáhá tak předcházet ohrožení dat malwarem.



Ochrana serveru Exchange

Testuje a filtruje e-maily na úrovni serveru Exchange, čímž pomáhá zastavit potenciální útoky ještě předtím, než se rozšíří do sítě.



Online zabezpečení a soukromí



Ověřené weby

Tato funkce podporuje bezpečnější procházení webu a používání bankovníctví, protože vašim zaměstnancům pomáhá vyhnout se falešným webům, jejichž cílem je krádež citlivých údajů, jako jsou uživatelská jména, hesla a údaje o platebních kartách. Je navržena tak, aby chránila uživatele před zneužitím DNS (systému doménových názvů).



Bezpečnostní rozšíření prohlížeče

Kontroluje reputaci a hodnověrnost webů, blokuje reklamy a zlepšuje ochranu soukromí tím, že zařízení uvede do „super bezpečného režimu“.



Čištění prohlížečů

V prohlížečích hledá doplňky se špatnou reputací a pomáhá mazat soubory cookie s osobními údaji.





Ochrana hesel

Pomáhá chránit přihlašovací údaje zaměstnanců uložené ve webových prohlížečích před odcizením a zneužitím. Je navržena tak, aby bránila aplikacím a malwaru v manipulaci s hesly uloženými v prohlížečích Google Chrome, Mozilla Firefox, Microsoft Edge a Avast Secure Browser.



Štít webové kamery

Brání aplikacím a malwaru v přístupu k webové kameře počítače bez souhlasu uživatele. Štít webové kamery znemožňuje nedůvěryhodným aplikacím pořizování obrázků nebo videí a narušování soukromí uživatelů.



Flexibilní správa zařízení

Zvolte si možnost správy, která je pro vaši firmu nejvhodnější.

Online platforma pro správu

Přímo ve webovém prohlížeči získáte přehled o kybernetických hrozbách v reálném čase, komplexní reporty a funkce pro správu. Naše cloudová konzole umožňuje centrálně spravovat bezpečnostní služby Avast Business a jejich předplatná.

Bez možnosti správy (individuální instalace)

Ideální pro malé kanceláře, které nepotřebují funkce centrální správy. Uživatelé mohou nastavení zařízení přizpůsobit svým požadavkům a mají úplnou kontrolu nad svými daty.

Místní správa není k dispozici.

Funkce Avast Business Hubu (online platformy pro správu)

- Intuitivní řídicí panel
- Komplexní reporty
- Správa zařízení a pravidel
- Centralizované výstrahy a oznámení
- Příkazy v reálném čase
- Zjišťování v síti a vzdálené nasazení
- Základní nástroj pro vzdálený přístup a podporu
- Podpora více tenantů

Integrované služby (dostupné jako doplňky v Business Hubu)

- Správa oprav
- Prémiové vzdálené ovládání
- Zálohování v cloudu

O Avast Business

Avast dodává intuitivní, cenově dostupná a oceňovaná řešení kybernetického zabezpečení pro malé a rostoucí firmy. Avast poskytuje integrované bezpečnostní služby pro ochranu zařízení, dat, aplikací a sítí. Díky 30 letům inovací máme jednu z největších a globálně nejrozsáhlejších sítí pro detekci hrozeb na světě. Naše řešení kybernetického zabezpečení jsou vytvořena tak, aby poskytovala maximální ochranu, takže se nemusíte tolik obávat kybernetických hrozeb a můžete se více soustředit na rozvoj své firmy. Další informace o našich řešeních kybernetického zabezpečení najdete na stránce www.avast.com/business.