Společnost **Barracuda Networks**, sídlící v Silicon Valley, působí celosvětově s více než 1 500 zaměstnanci a nabízí špičková, komplexní a cenově dostupná řešení v oblasti zabezpečení IT. Ve více než 225 000 organizací po celém světě, od malých a středních podniků po velké společnosti, pomocí inovativních řešení zabezpečuje ochranu e-mailů, chrání firemní aplikace a cloudová řešení, zabezpečuje sítě a chrání firemní data.

Barracuda Networks je partnerem Amazon Advanced Technology Partner a **Microsoft Partner of the Year Winner** (cena za řešení ISV s certifikací Microsoft Azure) a pomohla desítkám tisíc zákazníků bezpečně přejít na Office 365 a Azure.

Společnost **Barracuda Networks** získala ocenění Comparably za **Best Company Culture** a byla také zařazena do seznamu do seznamu 25 nejžhavějších společností CRN 2021 **Edge Security Computing 100**.

Více na stránkách výrobce www.barracuda.com

EMAIL PROTECTION

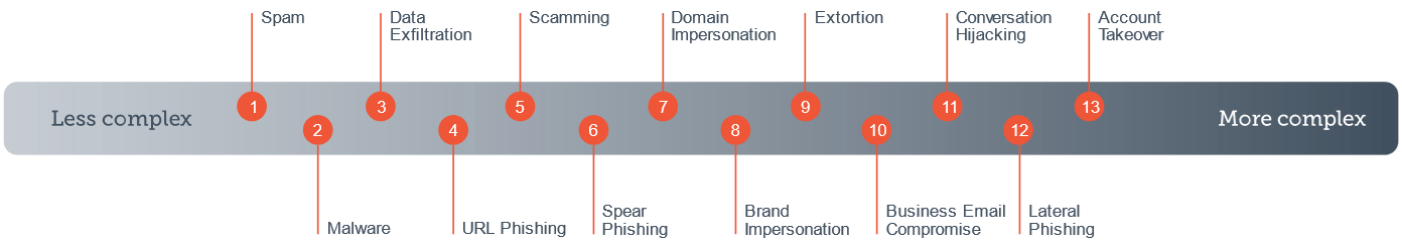
Zabezpečení e-mailu

Více než 91 % cílených kybernetických útoků začíná e-mailem.

E-mailové útoky jsou stále složitější a nebezpečnější. Mnoho e-mailových hrozeb dnes využívá taktiky sociálního inženýrství k cílení na uživatele a obcházení e-mailových bezpečnostních bran. Chcete-li chránit své podnikání a data, musíte zůstat napřed kyberzločinci.

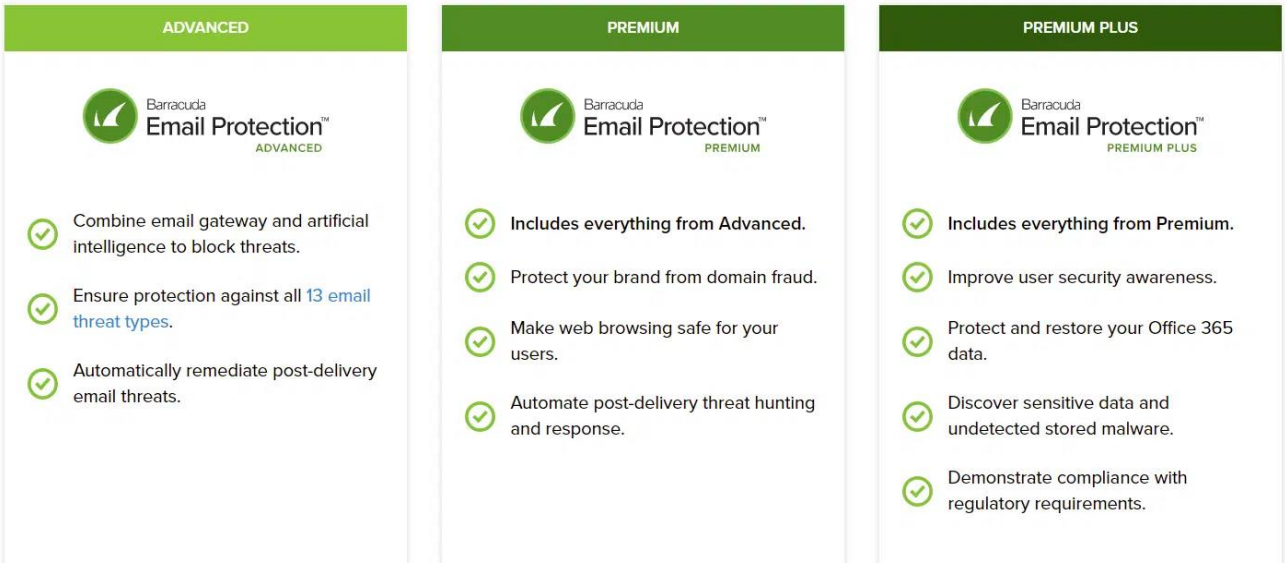
Pouze Barracuda chrání před všemi 13 typy e-mailových hrozeb.

Barracuda Email Protection poskytuje **nejkomplexnější** ochranu proti všem 13 typům e-mailových hrozeb, od spamu a ransomwaru až po sociálně inženýrské hrozby, jako je spear phishing, kompromitace firemních e-mailů a převzetí účtu.



Ochrana e-mailů vyžaduje více vrstev ochrany. Většina řešení ochrany e-mailu se skládá pouze z e-mailové brány, která dokáže odfiltrovat některé typy e-mailů, aby se nedostaly na váš poštovní server. Barracuda kombinuje obranu brány s ochranou doručené pošty s umělou inteligencí pro ochranu před všemi typy e-mailových hrozeb.

Barracuda kombinuje svou globální databázi o hrozbách a umělou inteligenci k zastavení e-mailových hrozeb. Shromažďuje data o e-mailech, sítích a aplikacích od více než 200 000 společností po celém světě. Modul umělé inteligence analyzuje komunikační chování, aby v reálném čase detekoval a zastavil útoky. To znamená, že můžete použít informace o hrozbách k zablokování přístupu ke škodlivému obsahu a zajistit tak bezpečné procházení webu pro vaše uživatele.



Společnost SE Labs ocenila společnost Barracuda jako "**Nejlepší službu zabezpečení e-mailu**".

Nezávislá testovací společnost SE Labs se sídlem ve Velké Británii vyhlásila vítěze za rok 2021 Annual Awards společnost Barracuda v kategorii "Nejlepší služba pro zabezpečení e-mailu".

Společnost Barracuda byla vybrána jako vítěz ocenění **Best of Cybersecurity Awards** společnosti Expert Insights za podzim 2021.

EMAIL PROTECTION ADVANCED OBSAHUJE:

Barracuda Email Security Gateway

Ochrana před hrozbami přenášenými e-mailem.

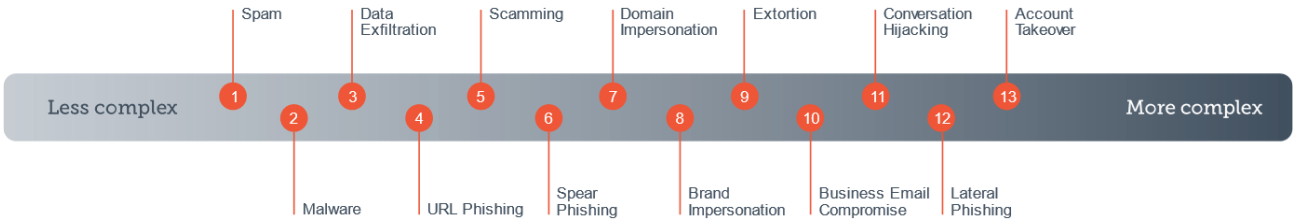
E-mail bezpečnostní brána Barracuda Email Security Gateway spravuje a filtruje veškeré příchozí i odchozí e-maily a ochraňuje tak organizace před hrozbami (včetně ransomware díky **integrované funkci ATP**) a úniky údajů šířených e-mailem. Některé z nejnebezpečnějších pokročilých hrozeb jsou navrženy tak, aby se vyhýbaly e-mailovým filtrům. Barracuda využívá Advanced Threat Protection jako cloudovou službu, která chrání proti ransomwaru a dalšímu malwaru, včetně zero-day útoků a pokročilých hrozeb.

Bezpečnostní brána Barracuda Email Security Gateway je k dispozici jako software pro virtuální platformy nebo software pro zabezpečení e-mailů ve veřejném cloudovém prostředí (Amazon Web Services (AWS), Microsoft Azure nebo VMware vCloud Air).

Chraňte se proti všem 13 typům e-mailových hrozeb

Přemýšlejte o ochraně proti všem 13 typům hrozeb i mimo bránu.

Chcete-li svou organizaci ochránit před útoky sociálních inženýrů, potřebujete další vrstvu obrany nad rámec emailové bezpečnostní brány – obranu na základě rozhraní API.



Ochrana proti spamu a malwaru

Chraňte svou firmu před e-mailovými kybernetickými hrozbami.

Zastavte spam a malware pomocí příchozího filtrování. Barracuda rychle filtruje a dezinfikuje každý e-mail předtím, než je doručen na váš poštovní server, aby vás ochránil před e-mailovými hrozbami. Pomocí antivirového skenování, hodnocení spamu, analýzy záměrů v reálném čase, ochrany odkazů na URL, kontroly reputace a dalších technik vám Barracuda poskytuje nejlepší možnou úroveň ochrany.

Barracuda Central je globální operační středisko nepřetržitě fungující (24x7), zaměřující se na bezpečnostní hrozby, neustále monitoruje internet, zda neobsahuje nové hrozby napříč všemi vektory útoků, a předává tyto informace zpět k zákazníkům.

Ochrana příloh

Barracuda kombinuje behaviorální a heuristické technologie a technologie sandboxu k ochraně proti útokům zneužívajícím zero-day zranitelností a cíleným útokům. Prostředí sandboxu se používá k odzkoušení a pozorování chování podezřelých příloh v zabezpečené oblasti mimo prostředí zákazníka.

Ochrana odkazů

Ochrana odkazů automaticky přepisuje adresy URL tak, aby při kliknutí na odkaz mohla Barracuda provést sandbox a zablokovat škodlivé odkazy.

Kontinuita e-mailu

V případě výpadku poštovního serveru nebo ztráty konektivity umožňuje nouzová poštovní schránka uživatelům pokračovat v odesílání a přijímání e-mailů a zůstat produktivní, dokud nebudou primární servery opět online.

Šifrování e-mailů

Udržujte e-mailovou komunikaci v soukromí a bezpečí.

Nasazení samostatných služeb šifrování e-mailů může být natolik náročné na správu a používání. Barracuda poskytuje jednoduché šifrování e-mailů, které je mimořádně bezpečné a je součástí kompletního řešení ochrany e-mailů. Ještě důležitější je, že Barracuda kombinuje šifrování e-mailů s dalšími vrstvami ochrany dat, včetně prevence úniku dat, archivace a filtrování, které blokují malware a pokročilé hrozby.

Barracuda šifruje všechny e-maily a přílohy na každém serveru, kde se nacházejí. Pokud uživatel odpoví na zašifrovanou zprávu, je automaticky zašifrována i odpověď.

Použijte šifrování AES-256 s automatickou správou klíčů.

Barracuda používá k zabezpečení všech šifrovaných e-mailů 256bitové klíče, běžně známé jako AES-256. To je zásadní pro silně regulovaná odvětví, jako je zdravotnictví, finance a právní organizace, které musí zabezpečit určité kategorie dat. Pomocí řešení Barracuda můžete snadno vytvářet zásady pro automatické šifrování e-mailů na základě odesílatele, příjemce, klíčových slov, domény a mnoha dalších kritérií. To poskytuje bezpečný a spolehlivý způsob sdílení citlivých informací se zákazníky a partnery. Snižuje potenciální riziko ztráty dat a zároveň usnadňuje dodržování předpisů.

Prevence ztráty dat

Funkce DLP (Data Leak Prevention) automaticky kontroluje každý odchozí e-mail na citlivý obsah. Na základě obsahu může být e-mail automaticky zašifrován, umístěn do karantény nebo zablokován. DLP zajistí, aby nebyly odeslány e-maily obsahující citlivé údaje, jako jsou čísla kreditních karet, čísla sociálního zabezpečení nebo informace chráněné zákonem HIPAA. Funkce DLP (Data Leak Prevention) automaticky kontroluje každý odchozí e-mail na citlivý obsah. Na základě obsahu může být e-mail automaticky zašifrován, umístěn do karantény nebo zablokován.

Ochrana před phishingem a vydáváním se za někoho jiného

Získejte přímou integraci s Office 365, abyste zabránili personalizovaným podvodným útokům, které tradiční e-mailové brány nedokážou detekovat v reálném čase.

Phishingové útoky a útoky na předstírání jiné identity využívají taktiky sociálního inženýrství, aby přiměly uživatele e-mailu poskytnout přihlašovací údaje, zaplatit fakturu nebo sdílet citlivé dokumenty. Barracuda tyto cílené útoky rozpozná a zablokuje je. Ochrana proti phishingu a předstírání identity Barracuda funguje tiše na pozadí.

Identifikujte pokusy o předstírání jiné identity, než se dostanou k vašim uživatelům.

Barracuda AI používá metadata z interních, externích a historických e-mailů k vytvoření profilu identity pro každého uživatele Office 365. Profil identity používá e-mailové adresy, typy dokumentů, použitá jména, analýzu přirozeného jazyka (NLP) a další data, která definují jedinečné komunikační vzorce jednotlivce. Tyto naučené vzorce umožňují společnosti Barracuda identifikovat anomálie chování, obsahu a přesměrování odkazů v e-mailové komunikaci vaší společnosti. Tato ochrana v reálném čase chrání vaši doručenou poštu před spear phishingem, kompromitací firemních e-mailů, laterálním phishingem a dalšími cílenými hrozbami.

Odstraňte škodlivé zprávy a pokusy o zosobnění v reálném čase.

Barracuda Phishing and Impersonation Protection je unikátní v tom, že neustále hledá hrozby a automaticky zabezpečuje doručenou poštu. Když je nalezen neobvyklý nebo škodlivý e-mail, je odstraněn z doručené pošty dříve, než uživatel může se zprávou interagovat.

Ochrana proti převzetí účtu

Chraňte se před vnitřními a vnějšími útoky.

Převzetí firemních účtů představuje pro podniky významnou novou hrozbu. Hackeři získávají přístup k firemním e-mailovým účtům prostřednictvím ukradených přihlašovacích údajů a používají je k provádění následných cílených útoků, interně i proti externím cílům. Převzetí účtu nebo útoky pocházející z těchto účtů je téměř nemožné odhalit, protože nevyužívají techniky předstírání jiné identity – pocházejí z legitimního účtu a prezentují se, že pocházejí z důvěryhodného zdroje. Ve skutečnosti tradiční řešení zabezpečení e-mailu ani nesledují interní provoz a nemají žádný způsob, jak zastavit útok pocházející interně.

Zabraňte ztrátě přihlašovacích údajů a převzetí účtu.

Barracuda detekuje jak pokusy o převzetí účtu, tak útoky spuštěné z kompromitovaných účtů. Analýzou historických i příchozích dat AI identifikuje anomálie chování, obsahu a přesměrování odkazů ve vaší organizaci za účelem označení a karantény podvodných e-mailů. Je také schopen zabránit pokusům o kompromitaci přihlašovacích údajů zaměstnanců automatickým blokováním cílených phishingových e-mailů, které se pokouší získat hesla zaměstnanců.

Jakmile je e-mailový účet kompromitován a hackeři jsou uvnitř organizace, mohou se začít přesouvat dále a hledat kompromitaci hodnotnějších účtů. Útočníci monitorují a sledují aktivitu, aby zjistili, jak vaše společnost podniká, a používají tyto informace k zahájení útoků proti vašim partnerům a zákazníkům. Se službou Barracuda bude váš IT a bezpečnostní tým upozorněn na podezřelé chování v e-mailových účtech vašich uživatelů, včetně neobvyklých přihlášení, změn pravidel doručené pošty a škodlivých e-mailů odeslaných z interních účtů.

Převzetí účtu může být pro organizace zničující a po identifikaci musí být rychle napraveno. Správci IT musí zajistit, aby byl útočníkům zablokován přístup k napadeným účtům, aby byly identifikovány všechny škodlivé zprávy a příjemci byli upozorněni. S nástrojem Barracuda pro nápravu převzetí účtu mohou administrátoři odstranit všechny e-mailové útoky odeslané interně z kompromitovaných účtů a vydávat upozornění všem externím příjemcům. IT týmy jsou schopny rychle zablokovat hackery z kompromitovaných účtů, aby bylo zajištěno, že již nebudou používáni se zlými úmysly.

Automatická náprava

Všechny zprávy nahlášené uživateli jsou automaticky kontrolovány na přítomnost škodlivých adres URL nebo příloh. Pokud je zjištěna hrozba, jsou všechny odpovídající e-maily automaticky přesunuty z poštovních schránek uživatelů do jejich složek s nevyžádanou poštou.

Získejte svůj bezplatný sken nyní. Je to rychlé, bezpečné a nemá žádný vliv na výkon vašeho e-mailu.

https://www.barracuda.com/redirect/ets

Ocenění

Společnost Barracuda je v žebříčku **The Forrester Wave™** uvedena jako lídr pro 2021 v kategorii Enterprise Email Security.

Společnost Barracuda byla vybrána jako **vítěz v kategorii Best-of Phishing Simulation and Testing** v rámci ocenění Best of Cybersecurity Awards společnosti Expert Insights za podzim 2021.

Již pátým rokem v řadě byla společnost Barracuda oceněna jako **zlatý vítěz v kategorii Nejlepší dodavatel zabezpečení elektronické pošty**.

Distributor pro ČR a SR:
atlantis telecom spol. s r.o. | Štěrboholská 1427/55 | 102 00 Praha 10 - Hostivař
Telefon: +420 271 004 208 | http://www.atlantis.cz | networking@atlantis.cz