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.

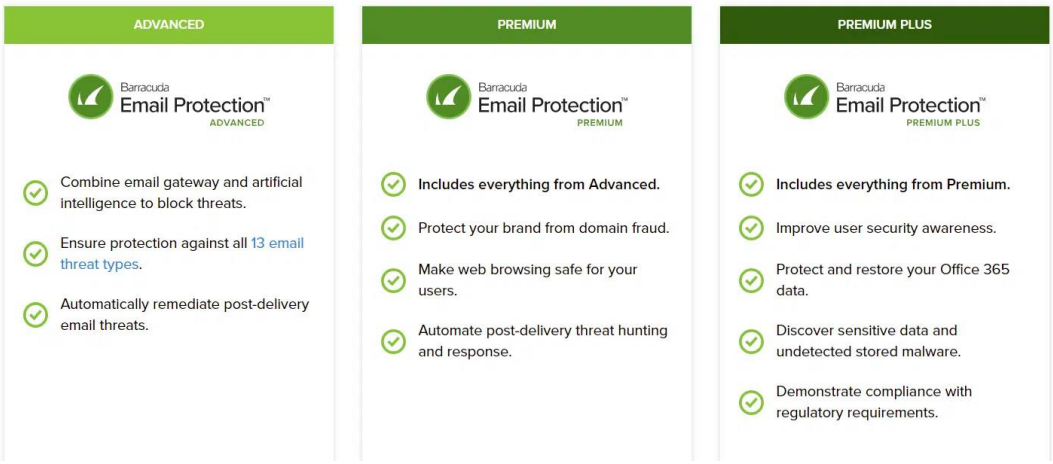
E-mailové útoky jsou stále složitější a nebezpečnější. Mnoho e-mailových hrozeb dnes využívá taktiky sociálního inženýrství k cílení na uživatele a obcházení e-mailových bezpečnostních bran. Chcete-li chránit své podnikání a data, musíte zůstat napřed kyberzločinci.

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 PREMIUM PLUS PLÁN OBSAHUJE:

Vše, co plán Advanced a Premium:

Ochrana proti spamu a malwaru

Ochrana příloh

Ochrana odkazů

Kontinuita e-mailu

Šifrování e-mailů

Prevence ztráty dat

Ochrana před phishingem a vydáváním se za někoho jiného

Ochrana proti převzetí účtu

Automatická náprava

Vyhledávání hrozeb a reakce na ně

Automatizované workflows [NOVINKA]

Integrace SIEM/SOAR/XDR [NOVINKA]

Ochrana domény před podvody

Filtrování DNS

Rozšířená o:

Archivace Barracuda Cloud

Průměrný uživatel e-mailu odešle a přijme přibližně 100 e-mailů denně.

Služba Cloud Archiving Service poskytuje **neomezené úložiště na uživatele**, čímž snižuje potřebu ukládat e-maily na serveru Exchange a v poštovních schránkách Office 365.

Indexovaný archiv poskytuje opakované, víceúrovňové vyhledávání a možnosti označování, které podporují komplexní audit a vyhledávání. Tím se výrazně zkracuje čas a snižuje úsilí potřebné k reakci na požadavky na zjišťování. Zajištění shody s předpisy.

Multifunkční doplněk aplikace Microsoft Outlook poskytuje integrované prostředí v jejich známém klientovi aplikace Outlook a umožňuje jim bezproblémovou práci s poštovní schránkou i archivovanými daty. Uchovává také místní mezipaměť archivovaných zpráv, aby k nim byl zajištěn nepřetržitý přístup i v době, kdy jsou offline.

Barracuda Cloud to Cloud BACKUP (zálohování)

Flexibilní, komplexní Podpora Office 365.

Barracuda Cloud-to-Cloud Backup nabízí rychlé zálohování, vysoce granulární možnosti obnovy a bezkonkurenční snadné použití.

Najděte a obnovte přesně ta data, která chcete, rychle a snadno pomocí nově přepracovaného uživatelského rozhraní, které je přístupné odkudkoli s připojením k internetu.

Podpora Office 365.

Barracuda Cloud-to-Cloud Backup vám poskytuje flexibilitu při obnově dat Teams, Exchange, SharePoint a OneDrive buď plně anebo s velmi podrobnými detaily. Plná podpora SharePointu znamená, že můžete zálohovat a obnovovat vše, co je na SharePointu, včetně různých šablon webů, vlastních seznamů, oprávnění a metadat – což eliminuje mnoho práce a nákladů spojených pouze s obnovou souborů. Zálohování a obnova poštovních schránek Exchange, veřejných složek a archivů nebylo nikdy jednodušší.

Zálohování Barracuda Cloud-to-Cloud nabízí kompletní, granulární ochranu vašich dat s možností vyhledávání v daném okamžiku a zálohování podle plánu i na vyžádání. Vaše data jsou navíc deduplikována a komprimována, aby se maximalizovala efektivita úložiště a minimalizovalo se zálohovací okno.

Zálohování do cloudu probíhá výhradně v cloudu, takže nemusíte spravovat ani aktualizovat žádný software ani hardware. Více externích kopií záložních souborů zajišťuje redundanci a bezpečnost.

Nasazení flexibilního a kompletního zálohování Office 365.

Doporučením číslo jedna od FBI, které pomáhá chránit se před útoky ransomwaru a jiného malwaru, je mít kvalitní zálohu dat. Společnost Microsoft také doporučuje používat pro zálohování dat Office 365 zálohy třetích stran, protože ty zajišťují pouze dostupnost služby, nikoli zálohování a obnovu dat.

Barracuda Data Inspector

Zabezpečte své prostředí proti nesprávně uloženým citlivým datům a skrytému malwaru a odhalte škodlivý software ve službě SharePoint a OneDrive.

Zabezpečte své prostředí před nesprávně uloženými citlivými daty a latentním malwarem. Přesvědčte se sami, jak Barracuda Data Inspector automaticky prohledává vaše data OneDrive pro firmy a SharePoint, zda neobsahují citlivé informace a škodlivé soubory. Zajistíte tak dodržování předpisů a snížíte rizika velkých regulačních pokut a poškození své pověsti.

Simulace útoku

Simulované phishingové útoky jsou neustále aktualizovány, aby odrážely nejnovější a nejčastější hrozby. Simulace se neomezují pouze na e-mailové útoky, ale zahrnují také hlasové útoky, útoky pomocí SMS a útoky na přenosná média (USB flash disk).

Školení o povědomí o bezpečnosti

Naučte své zaměstnance identifikovat potenciální bezpečnostní rizika a reagovat na ně pomocí školení Barracuda PhishLine. Zjednodušte povědomí o bezpečnosti a vyřešte tak zákonné požadavky na bezpečnostní školení zaměstnanců.

Barracuda Email Protection zastaví více než 20 000 spear phishingových útoků každý den. Školení bezpečnostního povědomí využívá tento obrovský zdroj útoků a hrozeb a slouží tak k vytvoření simulace útoků a školení v reálném světě v souladu se všemi identifikovanými 13 typy e-mailových hrozeb. Uživatelé se naučí odhalit kompromitaci firemních e-mailů, útoky na předstírání identity a další hlavní e-mailové hrozby.

Simulujte e-mailové hrozby.

Vyberte si ze stovek šablon hrozeb z reálného, převzatých přímo z rozsáhlé databáze hrozeb Barracuda, a vystavte své uživatele nejnovějším typům e-mailových hrozeb.

Analyzujte chování uživatelů.

Získejte podrobné metriky chování uživatelů, abyste mohli posoudit svá bezpečnostní rizika a informovat o svém přístupu ke školení.

Vzdělávejte se ke zmírnění rizika.

Vyberte si ze široké škály poutavého školícího obsahu navrženého tak, aby vyhovoval vašim jedinečným iniciativám v oblasti zvyšování povědomí.

Reakce na incidenty

80 procent organizací uvádí, že odpověď na e-mailové útoky trvá déle než 6 hodin.

Identifikujte anomálie, které mohou naznačovat hrozby, na základě poznatků získaných z analýzy dříve doručených e-mailů a informací získaných z komunity. Zabraňte budoucím útokům.

Když se útoky přenášené e-mailem vyhýbají zabezpečení a dostávají se do doručené pošty vašich uživatelů, musíte reagovat rychle a přesně, abyste zabránili škodám a omezili šíření útoku. Ruční reakce na útoky je časově náročná a neefektivní, což umožňuje šíření hrozeb a nárůst škod.

Barracuda Incident Response automatizuje tyto procesy, aby bylo zajištěno, že rychle identifikujete povahu a rozsah útoku, okamžitě odstraníte škodlivé e-maily a rychle provedete nápravná opatření, abyste zastavili postup útoku a minimalizovali škody.

Okamžitě reagujte na útoky přenášené e-mailem.

Když je experty z IT nahlášen škodlivý e-mail, Barracuda Incident Response vám umožní okamžitě prohledat všechny doručené e-maily podle odesílatele nebo předmětu a identifikovat všechny interní uživatele, kteří je obdrželi. Poté můžete automaticky odstranit všechny výskyty e-mailu obsahujícího hrozbu. Automatická náprava identifikuje a odstraní e-mailové zprávy, které obsahují škodlivé adresy URL nebo přílohy po doručení přímo z poštovních schránek uživatele bez vašeho přičinění.

Automatizujte celý proces reakce na incidenty.

Naše funkce **Automated Workflow** vám umožňuje vytvářet vlastní příručky a zcela automatizovat vaše reakce na různé e-mailové události v celé řadě řešení. Naše veřejná rozhraní API vám navíc umožňují integrovat data s vašimi platformami SIEM/SOAR/XDR za účelem zefektivnění operací a dalšího zachování zdrojů IT.

Barracuda Incident Response má výkonné analytické funkce, které vám umožňují používat poznatky získané z analýzy doručených e-mailů k identifikaci anomálií v e-mailech, které již jsou ve schránkách vašich uživatelů. Můžete například zkontrolovat geografické oblasti, odkud přicházejí příchozí e-maily, a proaktivně identifikovat škodlivé e-maily ze zemí, se kterými obvykle neobchodujete. Můžete stanovit priority a odhalit nové hrozby pomocí údajů o potenciálních incidentech souvisejících s těmi, které jste již vytvořili vy nebo jiní zákazníci Barracuda, a o hrozbách, které jsou aktuálně v oběhu a byly identifikovány zpravodajskými službami Barracuda. Tento přehled pomůže vašemu týmu identifikovat hrozby, které jinak zůstanou bez povšimnutí.

Integrovaná ochrana proti phishingu založená na doméně.

Barracuda Incident Response má také funkce pro zabezpečení obsahu, které nabízejí ochranu napříč e-mailem a webem. Detekuje a automaticky blokuje škodlivé domény obsažené v phishingových e-mailech pro všechny uživatele pomocí integrace API. Ochrana proti phishingu DNS funguje hladce a poskytuje jednotnou reakci správy hrozeb proti pokročilým útokům. Tato funkce je dostupná zákazníkům služeb Incident Response a Barracuda Content Shield.

98 % organizací s Office 365 uchovává škodlivé e-maily ve svých poštovních schránkách. Objevte e-mailové hrozby dříve, než je udělají vaši uživatelé.

Více než 11 000 organizací použilo skener k odhalení více než 7 milionů hrozeb, které se skrývají v jejich poštovních schránkách.

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

Barracuda byla oceněná jako celkový **vítěz v kategorii Data Protection and Management of the CRN's** 2021 Products of the Year.

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.