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

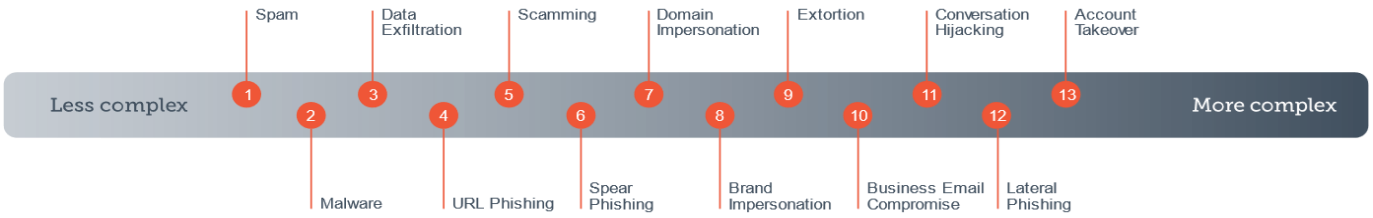
OCHRANA E-MAILU

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.

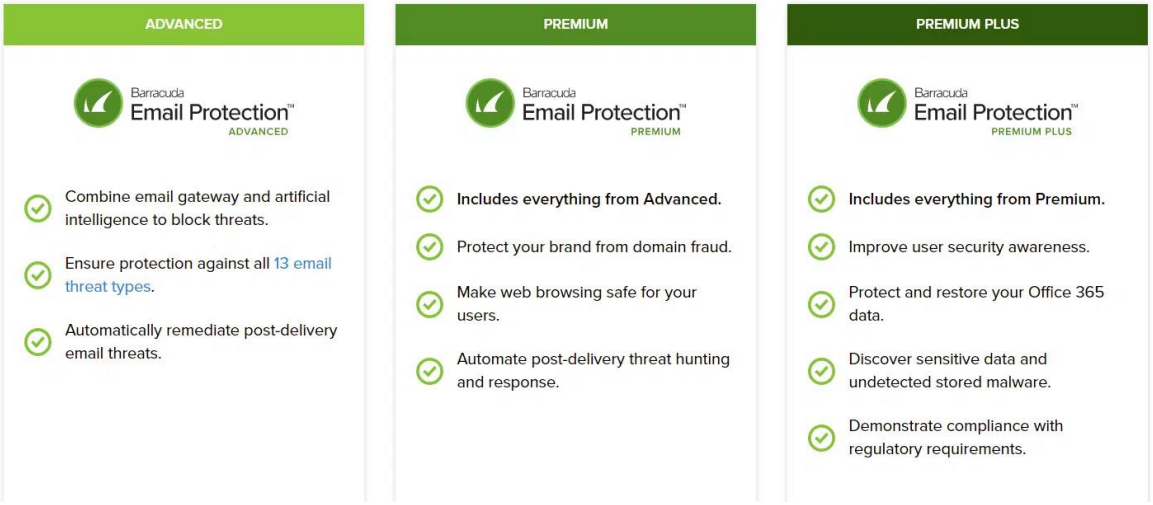
Pouze Barracuda chrání před všemi 13 typy e-mailových hrozeb.

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.

Ochrana proti spamu, malwaru a pokročilým hrozbám

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 zákazníků.

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.

Blokujte škodlivé e-mailové odkazy.

Hackeři a spammeři zahrnují do e-mailů odkazy, které klamou lidi, aby poskytli citlivé informace, nebo je přesunuli na škodlivý web, který by mohl šířit malware. Barracuda automaticky přepíše příchozí klamavou adresu URL v e-mailové zprávě a provede analýzu adres URL a domén v reálném čase v okamžiku kliknutí. Přepsané adresy URL neexspirují a fungují neomezeně dlouho.

Ochrana před ztrátou dat a šifrování e-mailů Barracuda zabrání tomu, aby citlivá data – jako jsou čísla kreditních karet, čísla sociálního pojištění, data HIPAA a další – opustila vaši organizaci. Zásady obsahu mohou automaticky zašifrovat, umístit do karantény nebo blokovat určité odchozí e-maily na základě jejich obsahu, odesílatele nebo příjemce.

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

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.

Zastavte spear-phishingové útoky pomocí zabezpečení doručené pošty řízené umělou inteligencí.

Barracuda kombinuje e-mailovou bránu s přímou API integrací do vašeho prostředí **Office 365**. Tato integrace poskytuje každému jednotlivci v organizaci přehled o interní, externí a historické e-mailové komunikaci. Umělá inteligence (AI) společnosti Barracuda využívá tyto zprávy k tomu, aby se naučila komunikační vzorce v rámci společnosti a mezi zaměstnanci. Architektura API umožňuje ochranu proti phishingu a předstírání identity identifikovat a blokovat útoky v reálném čase bez dopadu na výkon e-mailu nebo sítě.

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 grafu identity pro každého uživatele Office 365. Graf 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.

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.

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 z 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.

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

Ochrana domény před podvody

Globální DMARC Adoption, 2019 - Chraňte své značky před falšováním a předstíráním identity.

Spoofing domény a únos značky jsou běžné techniky používané hackery při útocích sociálního inženýrství. Mohou být použity nejen k cílení na vaše zaměstnance, ale také na vaše zákazníky, externí partnery a další třetí strany, které důvěřují vaší značce. Tyto útoky na předstírání identity mohou vést k finančním ztrátám a také k velkému poškození pověsti vaší značky.

DMARC (Domain-based Message Authentication Reporting and Conformance) **je standard** (který doporučuje NUKUB) pro ověřování e-mailů, který byl vytvořen za účelem blokování falšování domény, takže útočník nemůže použít značku vaší společnosti k předstírání identity a zahájení útoků. Jeho vymahatelnost poskytuje mechanismus pro automatické odmítnutí e-mailů, které nejsou odeslány z vašich legitimních e-mailových systémů. Barracuda's DMARC vám dává kontrolu nad vaší značkou a blokuje tyto útoky na zosobnění.

Barracuda poskytuje hlášení DMARC, které organizacím pomáhá správně nastavit prosazování DMARC a snižuje potenciál falešně pozitivních vynucení, jako je blokování legitimních e-mailů nebo nesprávná identifikace legitimního odesílatele.

Zajistěte doručitelnost svého e-mailu a získejte lepší návratnost investic do marketingu.

E-mailové kampaně fungují pouze v případě, že zákazníci vidí vaše zprávy. Odeslání e-mailu bez ověření DMARC zvyšuje riziko, že bude falešně identifikován a filtrován jako spam.

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

Filtrování DNS

18,5 milionu webových stránek je v každém okamžiku infikováno malwarem.

Kyberzločinci používají e-mail k doručování odkazů na škodlivé weby, ke kterým mají uživatelé přístup mimo váš poštovní systém – které se pak mohou rychle šířit.

Chraňte své uživatele e-mailu a síť před škodlivými adresami URL.

Barracuda Email Protection má integrovanou DNS Filtering, aby zajistila, že když zablokujete e-mailový útok, okamžitě také zablokujete všem svým uživatelům přístup ke stejnému škodlivému obsahu kdekoli ve vaší síti. Poskytuje také pokročilé filtrování DNS, aby uživatelům zabránilo v přístupu ke škodlivému webovému obsahu, který přichází prostřednictvím e-mailu nebo jiných komunikačních kanálů, včetně Slack a Microsoft Teams.

Nasaďte ochranu, kterou lze snadno spravovat a škálovat.

Integrované filtrování DNS Barracuda Email Protection je 100% služba (SaaS), což eliminuje složitost a náklady na tradiční nasazení hardwaru. Nastavení trvá pouhé minuty a jeho architektura bez proxy směruje k analýze pouze nedůvěryhodné požadavky, takže získáte optimální ochranu bez latence. Centralizovaná správa poskytuje okamžitý přehled o aktivitě prohlížení, což usnadňuje identifikaci rizik zabezpečení a dodržování předpisů.

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.

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.

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.

Šifrování e-mailů a prevence ztráty dat

Udržujte e-mailovou komunikaci v soukromí a bezpečí.

Nasazení samostatných služeb šifrování e-mailů může být natolik náročné na správu a používání, že se mnoho uživatelů rozhodne zásady bezpečné komunikace své organizace obejít. 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.

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.

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

Služba Archivace

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 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 snížili rizika velkých regulačních pokut a poškození své pověsti.

Získejte přehled o citlivých datech.

Užijte si snadnou a intuitivní správu zabezpečení dat bez hardwaru nebo softwaru. Identifikujte rizika na první pohled.

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. Jako komplexní řešení pro e-mailovou správu, Barracuda Email Security Gateway umožňuje organizacím šifrování zpráv a využívá cloud k uchování e-mailů, pokud se poštovní server stane nedostupným. 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).