DEEP SECURE

Deep Secure Content Threat Removal for Mail

E-mail bez hrozeb: snadno a jasně

Firemní uživatelé obvykle mají možnost používat e-mail a vyměňovat si ze svého pracoviště elektronickou poštu s uživateli uvnitř firmy i mimo ni. E-maily mohou obsahovat více než jen text – uživatelé často posílají přílohy a navíc používají formátování, odkazy, barvy a obrázky ve formátu HTML nebo Rich Text. Tím pro organizaci vzniká riziko, že přes e-maily pronikne do firmy škodlivý software ukrytý v jejich obsahu.

Tradiční e-mailové bezpečnostní brány spoléhají na odhalení potenciální hrozby a ukazuje se, že na současné sofistikované útoky prostě nestačí.

Hlavní výhody

Content Threat Removal for Mail

- Vždy přes hranici sítě doručí bezpečné e-mailové zprávy a přílohy bez hrozeb. Přitom není třeba hrozbu detekovat ani omezovat přístup uživatelů k obchodnímu obsahu, který potřebují. Všechny nově vzniklé hrozby, ransomware, steganografické útoky, malware šířící se bez pomoci souborů a hrozby obsažené v polymorfních souborech jsou odstraněny.

- Funguje spolu s vašimi stávajícími e-mailovými bezpečnostními branami, filtry spamu a antivirovým softwarem kontrolujícím okraj sítě. Toto řešení lze hladce začlenit do kybernetické ochrany síťové hranice, a s minimálním rizikem a nízkými náklady tak získat úplnou ochranu před hrozbami skrytými v obsahu.

DEEP SECURE

Braňte se před neznámou hrozbou

Stávající ochrana e-mailové komunikace na hranici sítě, tedy brány (spojující v sobě antivirovou ochranu, využívání informací o hrozbách, sandbox a filtrování spamu), představuje první obrannou linii. Podle signatur dříve odhalených útoků a nebezpečných chování odhalují známé hrozby. Společnosti jsou však znovu a znovu poškozovány nově vzniklými hrozbami, které do jejich sítě proniknou ještě předtím, než se o nich detekční obranné mechanismy dozví. Případně zcela neznámými hrozbami, kterým se podaří úspěšně zaútočit, aniž je vůbec někdo správně rozpozná.

Řešení Content Threat Removal for Email (Odstranění hrozby z obsahu e-mailů) je jediným způsobem, jak se ubránit nejenom známým, ale i dosud neznámým novým hrozbám, pronikajícím v e-mailu přes hranici sítě. Nespoléhá totiž na jejich detekci ani aktivaci v kontrolovaném prostředí sandboxu. Namísto toho unikátní transformační metodou zajišťuje naprostou ochranu.

Transformujte své zabezpečení e-mailu

Řešení Content Threat Removal for Mail nejprve z e-mailových zpráv a příloh, které jsou doručeny na hranici sítě, extrahuje obsažené obchodní informace. Data, kterými jsou tyto informace neseny, jsou odstraněna spolu s veškerými hrozbami. Pak jsou vytvořeny zcela nové zprávy a přílohy a doručeny uživateli. Od odesílatele k adresátovi se dostane jen bezpečný obsah. Útočník tak nepronikne obranou a firma přesto dostane, co potřebuje.

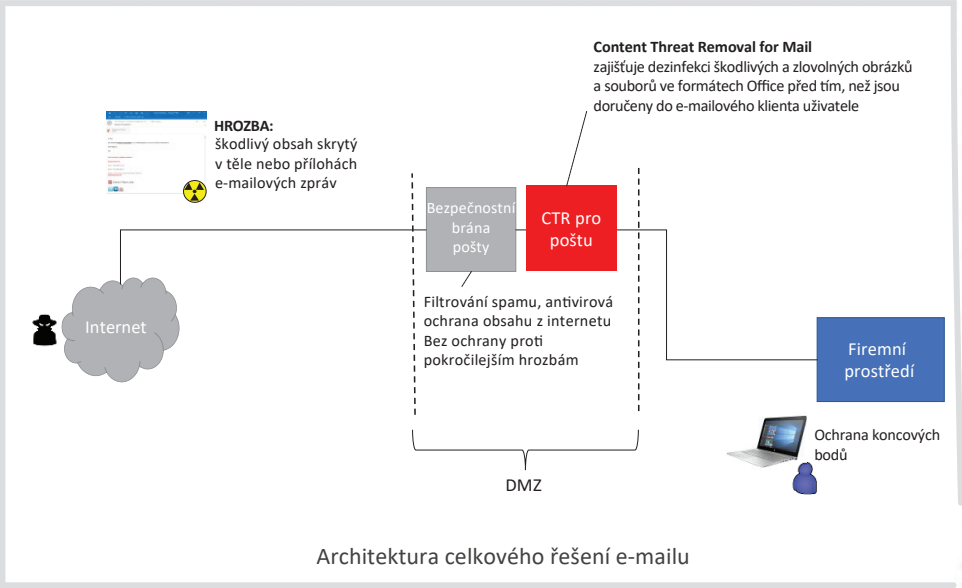
Tento postup se nazývá transformace. Nelze ho překonat. Bezpečnostní tým je spokojený, protože hrozby jsou odstraněny. A uživatelé jsou také spokojeni, protože dostanou potřebné informace.

Content Threat Removal je jediným způsobem, jak zaručit odstranění hrozeb z obsahu. Jedinečná technologie Content Threat Removal od firmy Deep Secure se oprostila od již překonaných paradigmat detekce a izolace hrozby a předpokládá, že nebezpečná jsou všechna data. Nesnaží se odlišovat dobrá od špatných.

Rozšiřte svoji stávající obranu

Řešení Content Threat Removal for Mail je rozšířením stávající e-mailové bezpečnostní brány a e-mailového serveru. Odstraňuje hrozby z těla e-mailových zpráv a příloh běžně používaných typů (obrázky, dokumenty Microsoft Office a PDF). Lze jej použít pro e-mailové systémy pracující na hardwaru zákazníka i v cloudu.

Řešení Content Threat Removal (CTR) pro poštovní brány doplňuje stávající zabezpečení e-mailu, protože představuje další prvek na cestě příchozího a odchozího e-mailového provozu.



Architektura celkového řešení e-mailu

DEEP SECURE

Deep Secure Content Threat Removal for Mail

Hladká integrace

Technologie Content Threat Removal for Mail v podobě nástroje pro Information eXchange (iX) funguje na firemním serveru za stávající e-mailovou bezpečnostní branou. Příchozí e-maily jsou z e-mailové bezpečnostní brány odeslány platformě CTR for Mail, která je zcela transformuje. Tím je zajištěna nezávadnost jejich těl i příloh. Až poté jsou doručeny na firemní poštovní server, odkud si je mohou stáhnout firemní uživatelé.

Další riziko pro bezpečnost firemní sítě představují uživatelé, kteří potřebují přístup k firemnímu poštovnímu systému i z mobilních zařízení. Doplňkové řešení nazvané Deep Secure Content Threat Removal for Mobile Mail nicméně umožňuje mobilní přístup bez ohrožení firemního poštovního systému. Podrobněji se mu věnuje stručný popis řešení Deep Secure Content Threat Removal for Mobile Mail.

Zabraňte průniku malwaru skrze obsah

Nejčastějšími nosiči malwaru jsou v současnosti dokumenty Office, soubory Adobe Portable Document (PDF) a obrázky. Složitost těchto souborových formátů a aplikací, které s nimi pracují, z nich činí přirozený cíl útočníků.
Ať jde o jakýkoli škodlivý software – od ransomware a trojských koní z oblasti bankovnictví až po nástroje pro vzdálený přístup a záznamníky stlačených kláves – kybernetičtí zločinci vědí, že nejlepším místem, kam ukrýt nejnovější útok, je běžný obchodní dokument.
Obranu proti hrozbám pomocí konvenčního zabezpečení na základě detekce ještě více komplikují takové techniky, jako je bezsouborový malware a polymorfní metody.
A právě e-mail je výborným vektorem průniku.

Díky nástroji Content Threat Removal for Mail a jeho jedinečnému způsobu transformace e-mailů mohou firemní uživatelé používat elektronickou poštu zcela bez obav. Každý doručený dokument a obrázek prošel transformací a je zcela bez hrozeb.

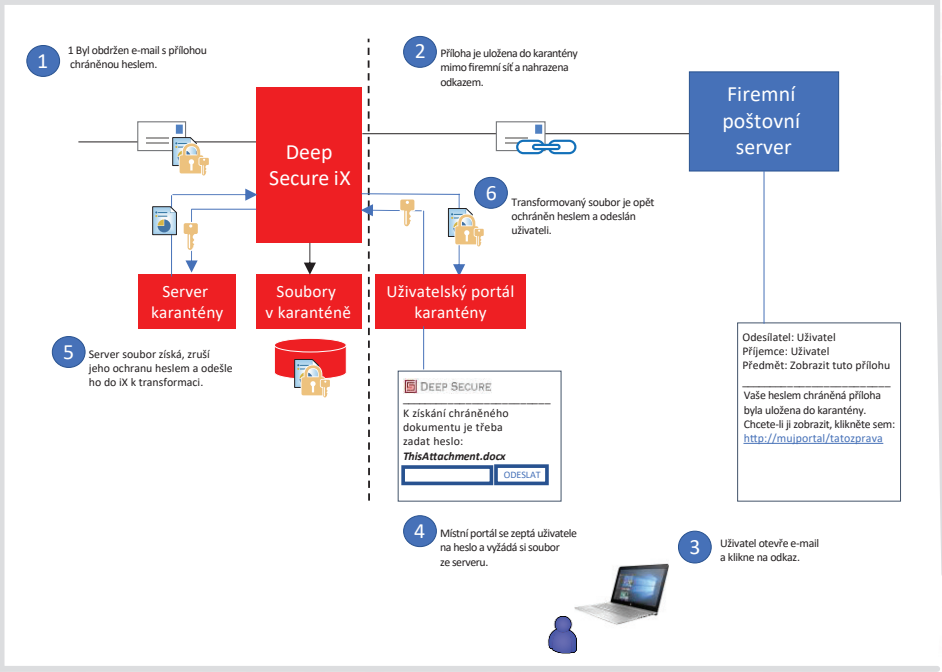
Proxy na aplikační vrstvě

Content Threat Removal for Mail funguje jako proxy server pro SMTP se dvěma rozhraními na aplikační vrstvě. Představuje bezpečnou hranici mezi firemní sítí a externími systémy. Funguje jako inteligentní hostitel bezpečnostní poštovní brány pro příchozí poštu a poštovního serveru pro odchozí poštu.
Veškerý obsah včetně MIME a příloh zpráv je transformován, takže pak může být bezpečně doručen do firemní sítě. Dále řešení provádí transformaci požadavků a odpovědí uživatelského portálu na přístup k heslem chráněným dokumentům uloženým v karanténě a transformaci heslem chráněných příloh získaných z karantény.

Content Threat Removal for Mail transformuje obdržený obsah na interní podobu obsažených informací. Původní data jsou zahozena a z informací jsou vytvořena nová „bezpečná“ data. Útoky nesené obsahem jsou tedy odstraněny, a to včetně těch neznámých, a informace se dostanou ke svému cíli. Tento postup je proveden pro veškerý přenášený obsah.

Deep Secure Personal Quarantine (PQ)

Deep Secure Personal Quarantine (osobní karanténa Deep Secure) uchovává heslem chráněné dokumenty. Uživatel z ní může soubory získat po zadání hesla. PQ je rozdělena na dva servery, každý na jedné straně hranice. Na firemní straně je uživatelský portál, který zpracovává žádosti uživatelů o přístup k heslem chráněným dokumentům uloženým v karanténě. Na vnější straně je server, který zajišťuje získání uložených dokumentů a jejich odeslání k transformaci.



Přílohy chráněné heslem

Uživatelé stále častěji chrání dokumenty posílané přes internet jako přílohy e-mailů heslem. Tyto šifrované dokumenty nemůže nástroj iX přímo transformovat, protože bez přístupu k obsahu z nich nelze získat obchodní informace. Takové přílohy jsou tedy uloženy do karantény mimo firemní síť a v e-mailech nahrazeny odkazy. Po kliknutí na odkaz může uživatel zadat heslo a získat bezpečnou verzi heslem chráněného souboru.

Podepsané a šifrované zprávy

Zprávy šifrované pomocí S/MIME nebo PGP nelze transformovat bez přístupu k šifrovacímu klíči. Budoucí verze nástroje Content Threat Removal for Mail budou podporovat ověřování podpisů a dešifrování obsahu před transformací. Transformované zprávy pak budou uživateli doručeny buď nepodepsané, nebo podepsané nástrojem iX a buď dešifrované, nebo znovu zašifrované.

Makra a spustitelný obsah

Nástroj Content Threat Removal for Mail standardně nepřenáší žádný spustitelný obsah ve zprávách ani jejich přílohách. Týká se to vložených binárních souborů, skriptů i maker.

Organizace nicméně často potřebují používat dokumenty s makry a sdílet je s externími uživateli. Vynechání těchto maker by mohlo způsobit ztrátu funkčnosti.
Pokud je podpora firemních maker potřeba, může správce v nástroji Content Threat Removal for Mail nastavit důvěryhodná firemní makra.

Při transformaci dokumentů s makry sice tento nástroj žádná makra ani spustitelný obsah z vnější strany nepřenese, nicméně označí dokument, v němž byla některá z firemních maker obsažena. Při obnovování obchodních informací pak známá bezpečná firemní makra do dokumentu vrátí.

Duální desktopy

V prostředích vyžadujících silné zabezpečení lze nástroj Content Threat Removal for Mail nasadit jako e-mailové řešení s dvojím desktopem. Uživatelé tak mají k dispozici druhý počítač mimo chráněnou síť, na němž mohou přistupovat k méně důvěryhodnému obsahu.

Při takovém nasazení mohou uživatelé bezpečným způsobem pracovat se soubory nepodporovaných typů a prohlížet si původní netransformované dokumenty.

DEEP SECURE

Vytvořte úspěšné řešení

Technická podpora Deep Secure vám pomůže zajistit bezproblémové nasazení i další provoz. Náš tým Solutions (Řešení) má rozsáhlé zkušenosti a má k dispozici nepřeberné množství informací, takže se na něj můžete spolehnout jako na přirozené rozšíření vašeho vlastního interního týmu.

Souhrn: Využívejte jedinečné ochrany

Stojíme na pokraji technologické revoluce. Tváří v tvář neúnavným a soustředěným kybernetickým útokům musí organizace přehodnocovat všechny aspekty toho, jak v digitálním světě získávají a sdílejí informace a provádějí transakce.

Obrana založená na detekci známých hrozeb je nedostatečná. Zabezpečení na bázi izolace a detekce v sandboxu omezuje činnost firmy a ponechává příliš mnoho náhodě. Skutečně potřebná je ochrana.

Řešení Content Threat Removal for Mail poskytuje jedinečnou ochranu firemních uživatelů. Zajišťuje, že zprávy a připojené obchodní dokumenty jsou s naprostou jistotou prosty všech hrozeb.

Další informace

Další informace o tom, jak řešení Content Threat Removal for Mail využívá produkt Information eXchange (iX) od společnosti Deep Secure, naleznete na adrese **www.deep-secure.com/products**.