Deep Secure Gateway eXtension (GX)

Chrání uživatele webu před známými, nově objevenými i neznámými hrozbami v obsahu. Zaručeně.

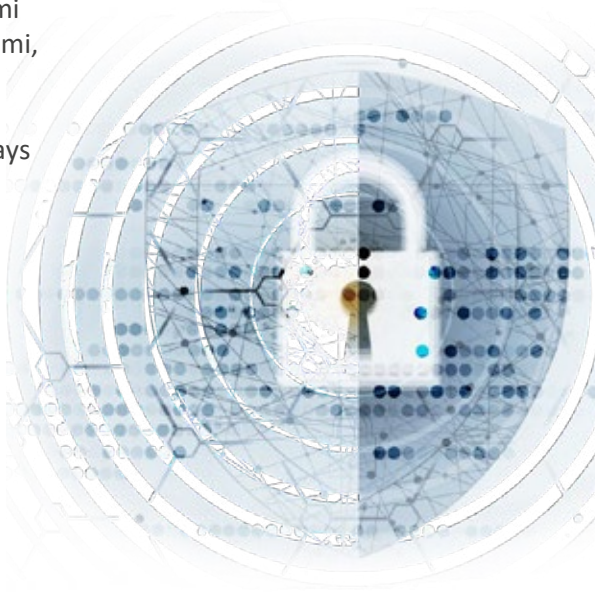
Stávající webové obrany síťové hranice (webové brány a firewally) se nedokáží vyrovnat s neustálým přívalem známých, neznámých a čerstvě odhalených hrozeb ukrytých v obchodních dokumentech a obrázcích. Rozšiřte schopnosti své hraniční obrany pomocí modulu Deep Secure Gateway eXtension (GX) a budete mít od těchto hrozeb klid. Zaručeně.

Už vás neohrozí ani nově objevené hrozby – zaručeně!

Modul Deep Secure Gateway eXtension pomocí metody odstranění hrozby z obsahu vždy doručuje bezpečný obsah bez hrozeb, aniž by hrozby potřeboval detekovat nebo izolovat uživatele od obchodního obsahu, který potřebují. Zastavíte ransomware, odrazíte i čerstvě objevené hrozby a odvrátíte steganografické útoky, aniž byste museli obsah zkoumat nebo se spoléhat na signatury. Ani ty nejpokročilejší cílené útoky a taktika nenápadného ztrácení dat nebudou mít šanci. Díky Deep Secure Gateway eXtension budete zcela chráněni před hrozbou nově vzniklých bezpečnostních útoků skrytých v obchodním obsahu.

Bezešvá integrace do stávající obrany

Deep Secure Gateway eXtension (GX) lze hladce propojit se stávajícími hraničními systémy pro ochranu webu, bezpečnými webovými branami, firewally nové generace a firewally webových aplikací, a to pomocí protokolu ICAP, který je v tomto oboru standardem. Je-li GX nasazen v rámci řešení Deep Secure Content Threat Removal for Web Gateways a Stegware Threat Removal for Web Gateways, přijímá obchodní dokumenty pomocí protokolu ICAP od vaší stávající hraniční obrany, transformuje je, přičemž z nich odstraňuje veškeré skryté hrozby, a vrací je zpět. Jde tedy o celkovou ochranu před hrozbami přenášenými obsahem, která má nízké náklady a minimální riziko.



Odstranění hrozeb z obsahu – digitální čistota

Jedinečná technologie transformace obsahu od společnosti Deep Secure předpokládá, že každý obchodní dokument nebo obrázek může obsahovat hrozbu. Na hranici sítě zachycuje obsah a na její druhé straně ho znovu od počátku vytvoří čistý a bezpečný. Tím je hrozba zničena. Od počátku ke konci se nedostane nic než bezpečný obsah. Uživatelé jsou při procházení webu v bezpečí a je zajištěno, že dokumenty, které přes web přenášejí, jsou v pořádku. A organizace se těší dobré pověsti pramenící z vědomí, že obchodní informace, které překračují její webovou hranici, jsou vždy digitálně čisté a bez hrozeb.

Boj proti steganografickým útokům

Steganografie skrývá data do zdánlivě neškodných souborů. Jde o způsob zakódování tajné zprávy do jiné zprávy, zvané nosič, aby ji mohl přečíst jen její zamýšlený příjemce. Steganografie se už dlouho používá k utajování komunikace před úřady. V poslední době je však na vzestupu takzvaný stegware, tedy využití steganografie kybernetickými útočníky. Pro IT odborníky je to špatnou zprávou, zvláště pro ty, kteří používají nástroje odhalující nebezpečná data. Steganografii totiž odhalit nelze. Díky řešení Deep Secure Gateway eXtension zničí vaše hraniční webová ochrana stegware skrytý v obrázcích. Ten tak nebude moci vnést do sítě malware, vynést ven cenná data ani umožňovat fungování ovládacích kanálů (CnC).

Forenzní analýza

Modul Gateway eXtension (GX) lze nastavit tak, aby zajišťoval podrobnou analýzu dat. Grafický řídicí panel poskytuje v reálném čase přehled obchodních dokumentů a obrázků, z nichž odstraňuje hrozby. Vyhrazená steganografická sekce obsahuje ukazatele pravděpodobnosti výskytu stegwaru v obrázcích. Možnost zobrazení podrobnějších údajů umožňuje snadno sledovat chování uživatelů při procházení webu. Pomocí pohledu „před a po“ pak mohou členové týmu SOC provádět forenzní šetření dokumentů a nalézt odpovědné uživatele. Informace pro audit a protokolování lze ukládat externě v datovém skladu organizace a je možno je zasílat systému SIEM.

Hlavní výhody

- Jednoduché nastavení – intuitivní grafické uživatelské rozhraní a (volitelná) předpřipravená integrace s nejznámějšími branami a firewally pomocí ICAP.
- Odstranění malwaru – hrozby skryté v dokumentech Office a PDF jsou během transformace odstraněny.
- Odstranění stegwaru – hrozby skryté pomocí steganografie ve webových obrázcích a zdrojích dat ze sociálních sítí (stegware) jsou během transformace odstraněny.
- Dvousměrná ochrana – zabraňuje v průniku malwaru, brání v úniku ukrytých dat a přerušuje kanály CnC.
- Audit a externí protokolování – umožňuje forenzní offline prověření.

Platformy

- Fyzická: Zařízení Deep Secure HRB
- Virtuální - minimální parametry: Paměť: 64 GB, Jader: 16, Disk: alespoň 80 GB
- V AWS

Operační systém

- Operační systém Deep Secure (DSOS)

Prohlížeč

- Jakýkoli prohlížeč kompatibilní s HTML5

Podporované typy souborů

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Adobe PDF
- Grafický formát GIF
- Grafický formát PNG
- Grafický formát JPG
- Grafický formát BMP
- Grafický formát TIFF
- JSON
- XML
- CSV
- ZIP
- TXT
- Rozšířená podpora při použití volitelného doplňkového příslušenství

Metody a algoritmus steganografického utajení

- Odhalitelná steganografie
- Neodhalitelná steganografie
- Nahrazení nejméně významného bitu
- Shoda nejméně významného bitu
- Vložení redundantních dat
- Uspořádání palety
- Uspořádání koeficientu F5 DCT

Datový sklad

- Možnost forenzní analýzy vyžaduje, aby zákazník zajistil vlastní podporu Amazon S3 a ES na svém zařízení nebo v cloudu.

Podpora integrace s branami a firewally

- GX lze nasadit spolu s jakoukoli webovou branou, firewallem nové generace a webovým aplikačním firewallem podporujícími ICAP.
- Propojení GX a McAfee Web Gateway verze 7.6.2 a novější pomocí ICAP bylo schváleno jako kompatibilní s McAfee.

Výkon

- Jedna fyzická instance podporuje 5000 uživatelů (při typickém využití k prohlížení webu).

Další informace

Další informace o způsobu nasazení GX v řešeních Content Threat Removal for Web Gateways a Stegware Threat Removal for Web Gateways naleznete na adrese **www.deep-secure.com/solutions**.