Deep Secure Policy Engine Guard

Chrání organizace před neúmyslnou ztrátou dat a napadením známým malwarem na hranici sítě.

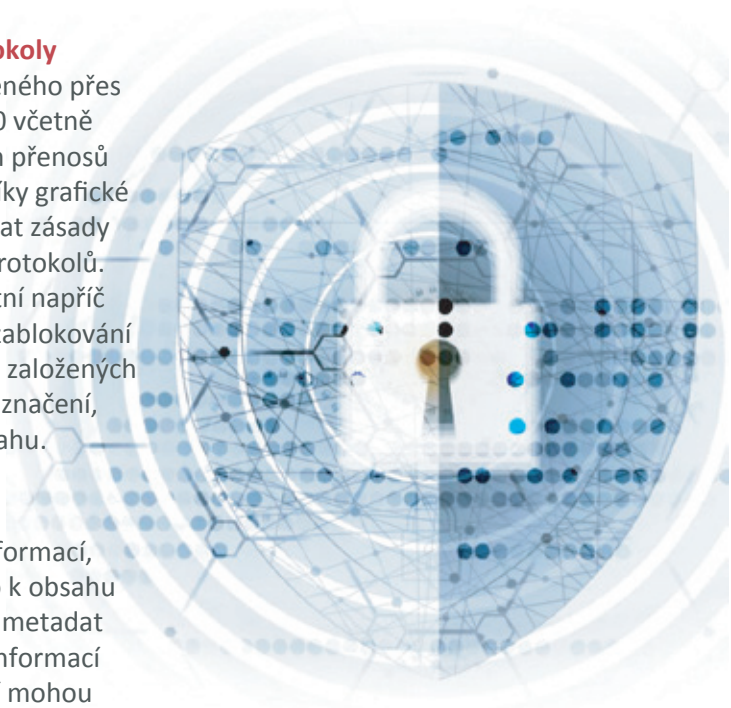
Nástroj Policy Engine Guard využívají organizace, které vyžadují přísnou kontrolu obchodního obsahu, který musí přecházet přes vnější hranici nebo mezi oddělenými interními zónami ve formě e-mailů, webové komunikace nebo přenosu souborů. Soustředí se na obchodní obsah a chrání před známým malwarem a neúmyslnou ztrátou dat. Ideálně se hodí pro systémy ve státní správě, pro orgány výkonné moci, obranné složky a kriticky důležitou národní infrastrukturu.

Hloubková kontrola obsahu

Policy Engine Guard zachycuje na hraničním bodu obsah a pomocí hloubkové kontroly obsahu (DCI) zjišťuje, zda v něm nejsou přítomny známé hrozby a zda nehrozí neúmyslná ztráta dat. Vložený obsah včetně archivů je rozbalen, takže systém získá úplný přehled o přenášených datech. Jsou zjištěny typy přenášených dat a těm, které jsou považována za rizikové, může být v překročení hranice zabráněno. Šifrovaná a chybně utvořená data jsou zablokována. Kromě toho lze kontrolovat provoz aplikačních služeb a ověřit tak, že je přenos dat náležitě omezen a odpovídá definicím předem určených schémat.

Konzistentní zásady bezpečnosti obsahu pro různé protokoly

Policy Engine Guard lze využít ke kontrole obsahu přenášeného přes hranici v podobě internetových e-mailů SMTP, zpráv X.400 včetně vojenských verzí, protokolů HTTP a HTTP(s) a souborových přenosů využívajících nástrojů Deep Secure pro přenos souborů. Díky grafické managementové konzoli je snadné modelovat a uplatňovat zásady bezpečnosti obsahu, které lze aplikovat na jeden či více protokolů. Bezpečnostní zásady organizace tak mohou být konzistentní napříč všemi vstupními a výstupními kanály. O propuštění nebo zablokování obsahu je rozhodnuto na základě velmi podrobných zásad založených na zdroji, cíli, uživateli, skupině, druhu obsahu, typu dat, označení, frázi a přítomnosti podepsaného a/nebo šifrovaného obsahu.



Špičková ochrana utajovaných informací

Policy Engine může identifikovat označení utajovaných informací, které odesílatel připojil k e-mailové zprávě či příloze nebo k obsahu přenášenému přes web. Toto označení může mít podobu metadat nebo viditelného textu, který udává citlivost příslušných informací nebo jakákoli zvláštní omezení nakládání s nimi. Označení mohou být zjišťována z první řádky textu zprávy, z jejího předmětu, hlaviček, digitálních podpisů, z vlastností dokumentu nebo z jeho záhlaví a zápatí.

Integrita a utajení

U e-mailu uplatňuje Policy Engine Guard pravidla pro ověřování adres a kontroluje, zda odesílatelova adresa patří do sítě, odkud zpráva přichází. Může také ověřovat signatury zpráv (S/MIME) a uplatňovat příslušná omezení podle toho, zda zpráva je či není podepsaná.

Systém může ověřovat zprávy šifrované pomocí standardu S/MIME, pokud odesílatel uvede Policy Engine Guard mezi příjemci kopie. Pravidla lze nastavit tak, aby byla zpráva v případě přijatelného obsahu doručena nebo aby byla před doručením dešifrována. To brání úniku citlivých informací ze systému.

Propojení sítí, které byly dříve považovány za nepropojitelné

Policy Engine Guard lze instalovat na platformu Bastion od společnosti Deep Secure, která propojuje dvě nebo více sítí pomocí samostatných síťových rozhraní. Zajišťuje důsledné oddělení sítí, a přitom umožňuje provoz mezi nimi. Díky tomu neexistuje žádné jiné riziko útoku ani úniku a zároveň lze propojit i sítě, které byly dříve považovány za nepropojitelné. Platforma Bastion je zvláště odolná proti přímým útokům. Používá pokročilé bezpečnostní mechanismy operačního systému Solaris 10 Trusted Extensions od firmy Oracle. Díky těmto mechanismům nelze nástroj Policy Engine a jím prováděnou kontrolu kritického obsahu nijak obejít. Jejich spolehlivost byla nezávisle potvrzena certifikací podle Common Criteria EAL4.

Hlavní výhody

- Podrobné zásady: podle zdroje, cíle, uživatele, skupiny, typu obsahu, označení, fráze a toho, zda obsah je či není podepsán
- Identifikace typu dat: uplatňování zásad podle typu dat
- Štítky: Zásady lze uplatňovat na základě označení nestrukturovaných či strukturovaných ochranných označení či bezpečnostních štítků a stupně prověrky uživatele
- Textová analýza: detekce slov nebo frází, kdekoli se v obsahu nacházejí
- Autentifikace: ověřování adres (e-mail) a NTLM autentifikace uživatelů (web)
- Integrita: ověřování zpráv podepsaných S/MIME (e-mail)
- Utajení: podrobná kontrola obsahu šifrovaných zpráv (e-mail) a prohlížení webu HTTP(s)

Platformy

- Fyzické: Platforma MRB001 Deep Secure je certifikována pro použití se systémem Oracle Solaris 10 (16 GB RAM, 2x 120GB pevný disk, 2x 6jádrový procesor Intel Xeon) a jakoukoli jinou hardwarovou platformou uvedenou na seznamu hardwaru kompatibilního s Oracle Solaris 10
- Virtuální: Minimální parametry: virtuální stroj VMware ESXi se 2 jádry, 2 GB RAM, 100GB pevným diskem a 2 síťovými kartami

Protokoly

- SMTP email
- X.400 e-mail včetně vojenských verzí
- DSFSP (protokol pro sdílení souborů Deep Secure)
- HTTP(s)

Operační systém

- Solaris 10 (volitelně s rozšířením Trusted eXtensions (TX))
- CentOS 6 or 7

Grafické uživatelské rozhraní pro správu
- Grafická konzole Clearpoint Windows

Hlavní oblasti zásad
- Kontrola protokolu
- Kontrola typu MIME
- Kontrola zdroje a cíle
- Omezení velikosti
- Podpis a šifrování podle S/MIME
- Kontrola typu dat
- Filtrování maker
- Textová analýza
- Ověřování schématu XML
- Bezpečnostní označení

Kontrola bezpečnostních označení
- Podporuje označení šifrovaná pomocí S/MIME ESS, P772, X.411 a ASN.1 a šifrovaná označení v předmětu, prvním řádku textu, metadatech a textu záhlaví či zápatí
- Podporuje překlad a mapování mezi různými schématy označování

(Volitelně) Propojení s antivirovým softwarem
- Sophos
- McAfee

Upozornění, sledování a audit
- Upozornění pomocí SNMP a SMTP
- Vestavěné protokolování umožňuje propojení se systémy SIEM
- Funkce podporující audit souladu s předpisy a vyšetřování – až na úroveň jednotlivých uživatelů