

PRÍRUČKA PREDAJA PRE PARTNEROV



POKROČILÉ HROZBY V SÚČASNOSTI sa vyvíjajú – ich taktika sa každým okamihom zdokonaľuje. Podľa najnovšej správy agentúry Forrester sa 53 % lídrov v oblasti podnikovej bezpečnosti vyjadrilo, že najväčšiu výzvu, ktorej ich spoločnosti čelia, predstavuje rýchly pokrok kybernetických hrozieb.¹

Aby vaši zákazníci mohli s týmto vývojom držať krok, potrebujú komplexnú ochranu siete, ktorá sa bude rozprestierať nad celou ich infraštruktúrou a ktorá bude predvídať zraniteľnosti v rámci všetkých možností útoku. Iba spoločnosť Fortinet ponúka úplnú architektúru end-to-end na inteligentnú, automatizovanú a účinnú bezpečnosť od dátovej centrály až po cloud – naprieč všetkými aplikáciami, používateľmi a údajmi.

V tejto príručke predaja predstavíme riešenie Fortinet Security Fabric pre zákazníkov a v krátkosti zhrnieme jednotlivé hlavné integrované riešenia. V každej kapitole uvedieme kľúčové hybné faktory riešenia, zhrnieme charakteristické vlastnosti produktu a poskytneme príslušné odporúčania k umiestňovaniu produktu („positioning“) a k predaju.

¹ Správa agentúry Forrester – “[Zamerajte bezpečnosť na pokročilé technológie](#),” júl 2017.

OBSAH

ÚVOD	4
NAŠE RIEŠENIA	5
SIEŤOVÁ BEZPEČNOSŤ	6
SECURE SD_WAN	14
MULTICLOUDOVÁ BEZPEČNOSŤ	21
BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ	29
E-MAILOVÁ BEZPEČNOSŤ	36
OCHRANA PROTI POKROČILÝM HROZBÁM	43
BEZPEČNÝ JEDNOTNÝ PRÍSTUP	52
BEZPEČNOSŤ KONCOVÝCH BODOV	59
SPRÁVA A ANALÝZA	66
SLUŽBY	72
NÁSTROJE PREDAJA	73
ŠKOLENIE	74
PARTNERSKÁ PODPORA	75

ÚVOD

Okrem neustále sa meniaceho prostredia hrozieb sa vaši zákazníci stretávajú aj s rýchlymi zmenami v rámci svojej vlastnej infraštruktúry. Aby mohli spoločnosti v súčasnej dobe úspešne konkurovať, podporujú digitálnu transformáciu (DX). Siete sa rýchlo vyvíjajú, aby aplikácie, dáta a služby mohli rýchlejšie prúdiť cez čím ďalej, tým rôznorodejšie prostredie používateľov, domén a zariadení.

Prirodzeným dôsledkom týchto pokrokov vo funkcionalite je, že moderné distribuované siete tak predstavujú oveľa širší priestor na útoky. Aj keď zariadenia IoT a aplikácie založené na cloude ponúkajú na jednej strane prevádzkové výhody, na druhej strane v značnej miere rozširujú priestor spoločnosti na útoky, ktorý je mimo dosahu a účinnosti predchádzajúcej generácie izolovaných bezpečnostných produktov. Tým možno vysvetliť skutočnosť, že 42 % lídrov v oblasti bezpečnosti uviedlo, že v ich spoločnosti došlo za posledné dva roky k narušeniu bezpečnosti.²

Spoločnostiam môže v boji s celou škálou výziev, ktorým sú v súčasnosti vystavené, pomôcť stratégia pripojenej bezpečnostnej architektúry medzi koncovými bodmi, ktorá sa prispôsobuje neustále sa vyvíjajúcim nárokom siete. **Systém bezpečnostnej architektúry Fortinet Security Fabric** poskytuje inteligentný architektonický prístup k bezpečnosti, ktorý podnikom umožňuje zviazať všetky svoje individuálne bezpečnostné riešenia do integrovaného celku. Náš systém bezpečnostnej architektúry je vystavaný na troch kľúčových atribútoch:

- **Šírka:** Pokrýva celý priestor na útoky. Bezpečnosť možno aplikovať na sieť, koncové body, IoT, prístup, aplikácie a cloud.
- **Integrácia:** Prepája rozdielne bezpečnostné riešenia a zjednodušuje komunikáciu, vďaka čomu sa znižuje čas detekcie a čas odozvy na realizáciu nápravy.
- **Automatizácia:** Umožňuje rýchlu a koordinovanú reakciu na hrozby. Všetky prvky si dokážu rýchlo vymieňať informácie o hrozbách a koordinovať svoju činnosť.

Tradičné, samostatné bezpečnostné riešenia pracujú v izolovanom priestore so samostatným riadiacim rozhraním bez zmysluplného spôsobu získavania či zdieľania informácií o hrozbách s inými zariadeniami v sieti. Neboli určené na ochranu dnešných distribuovaných architektúr naprieč všetkými vektormi útoku. Nedokážu ponúknuť dosah, výkonnosť ani synchronizovanosť reakcií, ktoré prirodzene poskytuje bezpečnostná spleť.

² Správa agentúry Forrester - "[Zamerajte bezpečnosť na pokročilé technológie](#)," júl 2017.

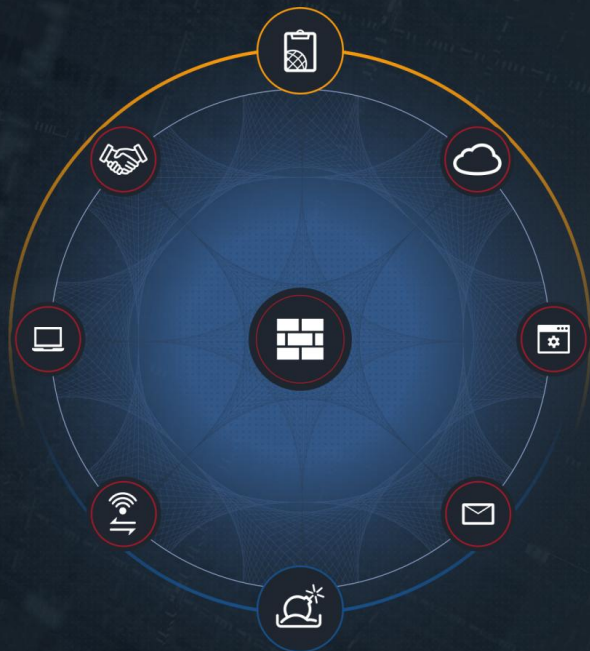
NAŠE RIEŠENIA

Systém Fortinet Security Fabric predstavuje pôsobivé riešenie, ktorým sa spájajú viaceré riešenia do integrovaného bezpečnostného rámca. Ak sa kdekoľvek v rámci podnikovej infraštruktúry nasadia bezpečnostné riešenia, musia pracovať rýchlosťou siete, aby sa ochranou neobmedzovala produktivita.

Riešenia Fortinet sú založené na najrýchlejších účelových **Security Processing Unit (SPU)** v odvetví, aby sa znížilo zaťaženie infraštruktúry a spoločnosti tak mohli zaviesť komplexnú bezpečnosť bez vplyvu na výkon. Obsahujú tiež softvérové optimalizácie a integrácie do cloudovej platformy na účel vyššieho výkonu v prostredí infraštruktúry ako služby (IaaS) a platformy ako služby (PaaS).

Okrem toho náš operačný systém FortiOS využíva výkonnostne optimalizovanú architektúru bezpečnostného systému na dosiahnutie rýchlejšej priepustnosti – až 10-krát vyššej ako pri rovnocenných riešeniach od iných dodávateľov. Posledná verzia systému, FortiOS 6.0, obsahuje viac ako 200 nových funkcií a vymožeností, ktorých účelom je pomôcť podnikom zrealizovať digitálnu transformáciu bez dosahu na výkonnosť siete či zníženie bezpečnosti.

Taktiež sa rozhodne hlásime k nezávislému testovaniu vykonávanému tretími stranami, aby sme ukázali, čo môžu spoločnosti očakávať od výberu bezpečnostných produktov značky Fortinet. Do tejto kategórie patrí účasť v širokej škále testov bezpečnostnej účinnosti v reálnom svete realizovaných inštitúciami ako napríklad NSS Labs, Virus Bulletin, ICSA Labs a AV-Comparatives.



SIETOVÁ BEZPEČNOSŤ

Kybernetickí zločinci pokračujú v automatizovaných a prepracovaných útokoch proti spoločnostiam, čím ohrozujú samotné základy digitálnej transformácie a účinnú realizáciu obchodných aktivít. Riziko narušenia (DX) dát burcuje spoločnosti, aby pridávali na sieťový perimeter viac bezpečnosti a viditeľnosti. Mnohé podniky však v súčasnosti využívajú bodové bezpečnostné riešenia, ktoré pri ochrane nechávajú medzery, ale zvyšujú pritom komplexnosť správy.

Jadro riešenia Network Security tvorí bezpečnostná architektúra Fortinet Security Fabric, ktorá ponúka pokročilé obranné prvky v rámci celej podnikovej siete. Fortinet Network Security predstavuje najširšiu škálu podnikových firewallov v odvetví, ktoré poskytujú škálovanú segmentáciu, automatizované zosúladenie a realizáciu nápravných opatrení od pobočky cez dátovú centrálu až po cloud. Naše vysokovýkonné firewally využívajú analýzu hrozieb v reálnom čase, aby zabezpečili komplexnú ochranu a hlbokú viditeľnosť na ochranu siete pred známymi a neznámymi útokmi.

Vychádzajúc z triedy výrobkov FortiGate, ktoré predstavujú vlajkovú loď našej spoločnosti, systém Fortinet Network Security využíva jediný operačný systém, ktorý pracuje naprieč rozdielnymi prípadmi použitia v oblasti sieťovej bezpečnosti. Fortinet Network Security prináša špičkovú bezpečnostnú účinnosť v porovnaní s inými riešeniami v odvetví, bezkonkurenčný výkon a znížené nároky na správu.



TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Firewally novej generácie sú aj naďalej dôležitou súčasťou

Nakoľko sa priestor na útoky v podnikovom prostredí neustále rozširuje, firewally novej generácie (NGFW) zostávajú aj naďalej kritickým prvkom stratégie hĺbkovej obrany. Podľa inštitúcie NSS Labs podniky investujú do ochrany perimetra prostredníctvom NGFW, ktorá zohľadňuje požiadavky DX a znižuje vektory útoku, ktoré kybernetickí zločinci môžu využiť na narušenie ich prostredia.³

Kritická je prevencia, rovnako ako aj detekcia hrozieb

Väčšina podnikov sa usiluje o prevenciu známych exploitov, škodlivého softvéru a škodlivých webových stránok a tiež o elimináciu bodových produktov. Zároveň sa čoraz dôležitejšou súčasťou ponúk NGFW stáva detekcia neznámych hrozieb prostredníctvom technológie sandbox.

Rastie potreba kontroly šifrovanej premávky

Za posledný rok vzrástla šifrovaná premávka prostredníctvom protokolov HTTPS a SSL z menej než polovice celkovej sieťovej premávky na rekordnú hodnotu takmer 60 %.⁴ Väčšina podnikov šifrovanú premávku nedešifruje pre výkonové a prevádzkové nároky. Ale s rastúcim objemom malvéru skrytým v šifrovanej premávke bude veľmi dôležité, aby NGFW vykonávali kontrolu SSL pri vysokých rýchlostiach bez toho, aby tým dochádzalo k problémom pri výkone.

³ "NSS Labs vyhlasuje výsledky skupinových testov firewallov novej generácie za rok 2017," NSS Labs, 6. jún 2017.

⁴ John Maddison, "Manažérsky pohľad: Trendy v oblasti hrozieb za r. 2017," Fortinet, 29.12.2017.

RELEVANTNÉ PRÍPADY POUŽITIA

Riešenie **Fortinet Network Security** ponúka flexibilitu, ktorú možno nasadiť v dátovej centrále, na okraji siete alebo v jej jadre. Relevantné prípady použitia:



Firewall novej generácie (NGFW)

- poskytuje podnikovú bezpečnostnú bránu do internetu používanú na okraji kampusu a dátovej centrály
- kontroluje a rieši škodlivý obsah vo vysokorýchlostných zašifrovaných prúdoch dátovej premávky
- rozsiahla, jemne granularizovaná bezpečnostná politika umožňuje segmentáciu siete a lepšiu viditeľnosť, riadenie a zamedzovanie hrozieb
- uplatňuje bezpečnostné politiky s ultranízkou latenciou, granulárnym riadením a viditeľnosťou používateľov a zariadení pre tisíce nezávislých aplikácií
- prostredníctvom preverovania skutočného obsahu sieťovej premávky identifikuje a zastavuje hrozby so silnou prevenciou prieniku nad rámec portu a protokolu
- podporuje najnovšie vysokorýchlostné rozhrania pre meniace sa požiadavky na výkon aplikácií a flexibilný dizajn siete
- klastre s vysokou dostupnosťou dovoľujú zvyšovanie softvéru pri behu služby, čím sa umožňuje rýchle preberanie inovačných prvkov bez toho, aby dochádzalo k prerušeniam siete počas vykonávania údržby



Systém prevencie prieniku (IPS)

- v praxi osvedčená, nezávisle testovaná sieťová bezpečnosť umožňuje kritickým obchodným aplikáciám pokračovať v behu pri súbežnom poskytovaní ochrany zaradenej do sieťovej cesty na okraji dátovej centrály

- prostredníctvom nepretržite aktualizovanej databázy známych hrozieb a najlepších riešení svojej triedy na odhaľovanie a ochraňovanie pred závažnými zraniteľnosťami nultého dňa poskytuje vysokovýkonnú ochranu proti utajeným hrozbám na sieťovej úrovni
- škálovateľnosť relácie absorbuje vysoký objem sieťovej a používateľskej premávky pre internetovo a cloudovo orientované dátové centrály



Bezpečná virtuálna privátna sieť (VPN)

- ponúka rozmanité vysokorýchlostné rozhrania s konektivitou uplatniteľnou aj v budúcnosti pre rôzne štruktúry siete ako napríklad prepojenie do hub-and-spoke a prepojenie medzi dátovými centráľami
- flexibilné a rôznorodé riešenia IPsec VPN typu policy-based a route-based spĺňajú rôzne požiadavky na šifrovanie prenášaných dát
- vysoká dostupnosť založená na klastroch uchováva stav relácie počas failover-u, čím zabezpečuje pružnosť a zlepšenie používateľského zážitku
- zahŕňa vysokovýkonné šifrovanie a riešenie v škále tunela v kompaktnej veľkosti, čím umožňuje realizovať konštrukčné návrhy dátovej centrály priaznivejšie k životnému prostrediu



Bezpečná webová brána (SWG)

- chráni proti webovým útokom pomocou filtrovania URL, pričom poskytuje viditeľnosť a riadenie šifrovanej webovej premávky
- konsoliduje sieťové služby a služby bezpečnej webovej brány, znižuje komplexnosť a stláča celkové náklady vlastníctva (TCO)
- zdieľa informácie o hrozbách v reálnom čase, čím pomáha zabráňovať prepracovaným zero-day hrozbám

PRODUKTY SIEŤOVEJ BEZPEČNOSTI



FortiGate

**FIREWALLY NOVEJ
GENERÁCIE**

NGFW značky FortiGate využívajú účelové bezpečnostné procesory, vďaka čomu poskytujú najlepšiu ochranu proti hrozbám dostupnú v odvetví a bránia pred väčšinou známych a neznámych pokročilých kybernetických útokov.



FortiGuard

**PREDPLATITEĽSKÉ
SLUŽBY
BEZPEČNOSTI**

Vývojový tím FortiGuard každý deň vyvíja účinné protiopatrenia na ochranu viac ako 300 000 zákazníkov na celom svete. Poskytuje najčerstvejšie aktualizácie informácií o hrozbách pre služby, akými sú napríklad systémy prevencie prieniku (IPS), antivírus (AV), filtrovanie webu, botnet a sandboxing. Zákazníci si môžu zakúpiť predplatné pre jednotlivé služby alebo celé balíčky, ako napríklad Enterprise, UTM (jednotná správa hrozieb) a Threat Protection (Ochrana proti hrozbám).



FortiOS

**SIEŤOVÝ
OPERAČNÝ
SYSTÉM PRE
FORTIGATE (OS)**

FortiOS riadi všetky bezpečnostné a sieťové funkcie prostredníctvom jediného, intuitívneho operačného systému. Zlepšuje ochranu a viditeľnosť, pričom vďaka konsolidácii stoviek funkcií znižuje prevádzkové náklady a šetrí čas. FortiOS umožňuje víziu Fortinet Security Fabric na zvýšenú ochranu od IoT po cloud.

INÉ PRODUKTY



FortiManager

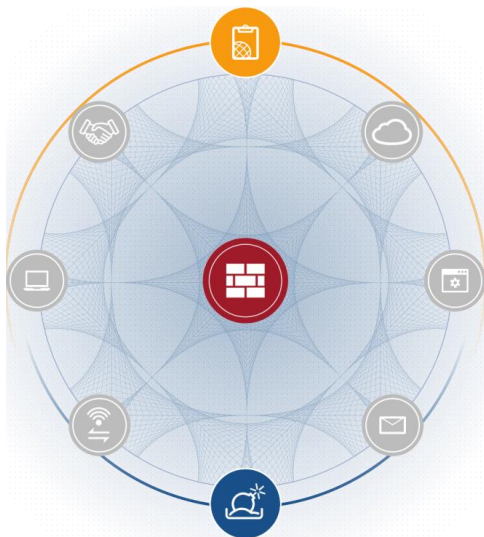
NOC-SOC prevádzkový nástroj, ktorý poskytuje centralizovanú správu a jednotnú politiku v rámci celej bezpečnostnej architektúry.



FortiAnalyzer

Ponúka kritický pohľad na hrozby a riziká a všade tam, kde sa vyžaduje okamžitá odozva.

FORTINET NETWORK SECURITY



Riešenie Network Security predstavuje jadro bezpečnostnej architektúry Fortinet Security Fabric. Umožňuje pokročilú bezpečnosť v rámci celého podniku s flexibilitou, ktorú možno použiť v dátovej centrále, na okraji siete alebo v jej jadre. Relevantné prípady použitia sú uvedené na pravej strane.

PREČO SÚ RIEŠENIA SIEŤOVEJ BEZPEČNOSTI FORTINET JEDINEČNÉ

Najlepšia bezpečnostná účinnosť v odvetví

Výskum FortiGuard Labs pomáha riešeniu Fortinet Network Security pri ochrane proti známym exploitom, škodlivému softvéru, aplikáciám a škodlivým webovým stránkam pomocou nepretržitého zberu a vyhodnocovania informácií o hrozbách. Taktiež pomáha detegovať neznáme útoky prostredníctvom dynamickej analýzy a poskytuje automatické zmierňovanie vplyvov na zastavenie cielených útokov. Fortinet sa neustále zúčastňuje na nezávislých certifikáciách vykonávaných napríklad inštitúciami NSS Labs, ICSA a Virus Bulletin a osvedčuje sa v nich na špičkovej úrovni efektivity.

Bezpečný procesor - poháňaný výkonom

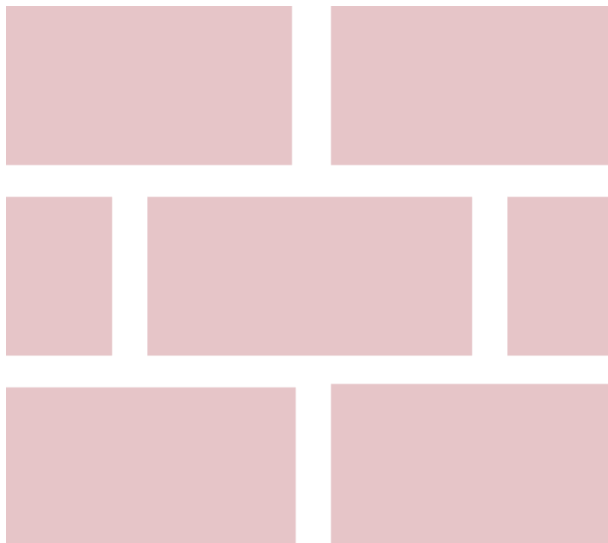
FortiGate NGFW poskytujú najlepšiu výkonnosť v oblasti ochrany proti hrozbám v odvetví s ultranízkyim reakčným časom. Takisto poskytujú špičkovú výkonnosť a ochranu v oblasti prevádzky zašifrovanej protokolom SSL. Produkty FortiGate neustále získavajú najvyššie hodnotenia pomeru cena/výkon v praktických skupinových testoch.

Výkon zabezpečovaný bezpečnostným procesorom

FortiGate NGFW ponúkajú najvyšší výkon IPsec v odvetví vďaka tomu, že využívajú technológiu účelových SPU. Umožňujú vysokovýkonný zašifrovaný prístup, agregáciu a konektivitu z dátovej centrálly na dátovú centrálu.

Jednoduchá a intuitívna správa

Produkty FortiGate ponúkajú najlepšie používateľské rozhranie v odvetví, pričom poskytujú 360-stupňovú viditeľnosť aplikácií, používateľov, hrozieb a všetkých topológií s cieľom rýchlej a intuitívnej identifikácie problémov. Na účely zlepšenia celkovej bezpečnostnej pozície taktiež disponujú preddefinovaným kontrolným zoznamom na dodržiavanie krokov, ktorý analyzuje nasadenie a zdôrazňuje zaužívanú prax.



KONKURENČNÉ POROVNANIE

Vlastnosť	Fortinet	Palo Alto Networks	Check Point	Cisco
Škálovateľnosť z okraja cez jadro k interným segmentom s rovnakou triedou produktov a OS	✓	častočne	✗	✗
Viditeľnosť a automatické odhaľovanie používateľov, koncových bodov, IoT a sieťových zariadení	✓	častočne	častočne	častočne
Najlepšia bezpečnostná účinnosť v odvetví vyhodnotená nezávislými tretími stranami (NSS Labs, ICSA, VB)	✓	častočne	✓	častočne
Výkon zabezpečovateľ bezpečnostným procesorom pri najlepšom pomere cena/výkon v branži	✓	✗	✗	✗
Single pane of glass a centralizovaná správa	✓	✓	častočne	✗

✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

Gartner 2017 Magic Quadrant pre Enterprise Firewalls – „Leader“

V teste Gartner Magic Quadrant pre Enterprise Firewalls od spoločnosti Gartner za rok 2017 urobil Fortinet výrazný posun z kategórie „Challenger Player“ do kategórie „Leader“.⁵ Firewally Fortinet FortiGate predstavujú ústredný prvok architektúry Fortinet Security Fabric – okrem poskytovania špičkovej funkcionality NGFW sú určené na zjednocovanie a automatizáciu viacvrstvových odpovedí na hrozby.



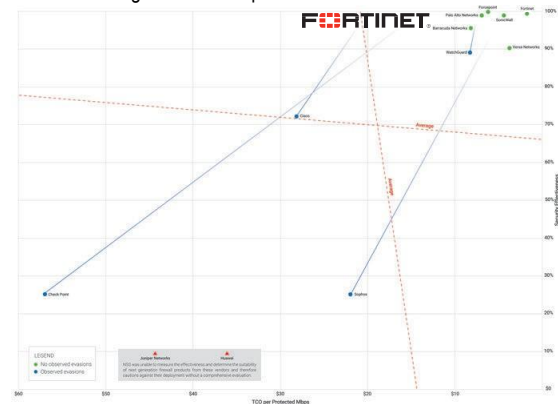
Magický kvadrant firewallov podnikových sietí od spoločnosti Gartner, Adam Hills, Jeremy D'Hoinne, Rajpreet Kaur, 10. júl 2017

Tento graf publikovala spoločnosť Gartner, Inc., v rámci väčšieho výskumného materiálu. Preto by sa uvedený graf mal posudzovať v kontexte celého dokumentu. Dokument od spoločnosti Gartner poskytne spoločnosť Fortinet na požiadanie.

Spoločnosť Gartner neschvaľuje žiadneho dodávateľa, produkt ani službu uvádzanú vo svojich výskumných materiáloch a ani neodporúča používateľom technológie, aby si vybrali iba tých dodávateľov, ktorí majú najvyššie hodnotenie či inú charakterizáciu. Výskumné materiály spoločnosti Gartner obsahujú iba názor výskumnej organizácie spoločnosti Gartner a nemajú sa chápať ako faktická skutočnosť. V súvislosti s uvedeným výskumom spoločnosť Gartner vylučuje všetky záruky, či už výslovné, alebo vyvoodené, vrátane akýchkoľvek záruk predajnosti či vhodnosti na určitý účel.

Porovnávacia správa a grafické hodnotenie NGFW od NSS Labs za rok 2018 – „Odporúčané“

V NGFW Comparative Report and Security Value Map za rok 2018 od NSS Labs získala značka FortiGate hodnotenie „Recommended“. Spoločnosť Fortinet poskytla na testovanie voči konkurenčným riešeniam svoj podnikový firewall FortiGate 500E, ktorý dosiahol vynikajúce hodnotenie bezpečnostnej účinnosti, keď pri nepretržitom testovaní v živom prostredí dokázal zablokovať 100 % únikov pri celkovom skóre 99,95 %. Produkt 500E tiež dosiahol vysoký výkon pri kontrole SSL, kde sa pri použití 32 šifrovacích súborov a novovytvorených šifier vyznačoval minimálnou degradáciou a neprekonanou účinnosťou.⁶



⁵ Adam Hills, Jeremy D'Hoinne a Rajpreet Kaur ["Magický kvadrant firewallov podnikových sietí"](#), Gartner, 10. júl 2017.

⁶ ["Bezpečnostná hodnotiacia mapa firewallov novej generácie \(NGFW\)"](#), NSS Labs, júl 2018.

HODNOTIACE OTÁZKY

- ☐ Mali ste nejaké problémy s narušením alebo incidenty v oblasti kybernetickej bezpečnosti?
- ☐ Máte obavy, že by nekalé elementy mohli v zašifrovaných tokoch skrývať škodlivý softvér? Obávate sa používať kontrolu SSL z dôvodu možného dosahu na výkon?
- ☐ Obávate sa o zabezpečenie a ochranu svojich podnikových aktív bez ohľadu na miesto ich inštalácie?
- ☐ Ochraňuje váš NGFW vaše interné siete od škodlivého softvéru a botnetov, ktoré sa už môžu nachádzať vo vnútri vašej infraštruktúry?
- ☐ Dokážete nasegmentovať vašu sieť na dosiahnutie jemne hladkej bezpečnostnej politiky tak, aby sa udržal ultranízky reakčný čas a zabezpečilo poskytovanie vysokoúčinnnej ochrany?
- ☐ Usilujete sa o konsolidáciu vašich sieťovobezpečnostných produktov s cieľom zníženia prevádzkovej zložitosti a s tým spojených nákladov?
- ☐ Máte hybridnú architektúru? Robíte si starosti ohľadom poskytovania rovnakých prvkov riadenia prístupu a ochrany prenášaných dát medzi aktívami, ktoré sú inštalované v priestoroch spoločnosti a v rámci viacerých cloudov?
- ☐ Robíte si starosti o spojenie s partnermi, dodávateľmi a poskytovateľmi? A čo prípady skrývania topológie, zhoršenia výkonu a bezpečnosti, ktorá nemusí byť úzko integrovaná so smerovaním?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Enterprise Firewall Solution
- NSE 3: FortiGate Mid-Range
- NSE 3: FortiGate High-End

SECURE SD-WAN

Prechod spoločností na digitálny obchodný model má výrazný vplyv na topológiu siete. Zavedenie cloudových služieb a ich využitie urýchľujú pokroky v široko pásmových sieťach WAN. Tradičný WAN sa považujú za drahé, komplexné a za riešenia s obmedzenými možnosťami. Nakoľko mnoho spoločností v súčasnosti zvažuje účinnejšie varianty WAN, kritickým faktorom sa stáva zavedenie nových bezpečnostných stratégií určených pre distribuovaný podnik.

Riešenie Fortinet Secure SD-WAN poskytuje bezpečnosť a sieťovú funkcionality novej generácie, ktorou sa zlepšuje efektívnosť WAN bez negatívneho vplyvu na bezpečnosť. Na rozdiel od tradičných architektúr dokážu nové softvérovo definované WAN dynamicky distribuovať premávku cez viaceré lokality, pričom automaticky reagujú na meniace sa aplikačné politiky. Umožňujú zákazníkom aktivovať priamy internetový prístup pre aplikácie SaaS na účel zlepšenia produktivity a nahradenia drahých spojení MPLS nákladovo priaznivejšími alternatívami.

Naše riešenie Secure SD-WAN zabezpečujú FortiGate Enterprise Firewalls, ktoré poskytujú vysoký výkon a špičkovú bezpečnosť proti rastúcej vlně kybernetických útokov v dôsledku priameho internetového pripojenia.



TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Rast zavádzania cloudových aplikácií

73 % spoločností tvrdí, že v roku 2020 budú skoro všetky ich aplikácie cloudové (SaaS).⁷ Zároveň väčšina týchto spoločností v súčasnosti zápasí s problémami latencie a výrazného poklesu viditeľnosti dát. Chcú sa vyhnúť sieťovému prenosu „backhaul“ z dátových centrál a chcú pre cloudové aplikácie začať využívať priamy internetový prístup.



73%

spoločností tvrdí, že v roku 2020 budú skoro všetky ich aplikácie cloudové (SaaS).

⁷ "Stav pracoviska s funkcionality SaaS," BetterCloud, prístup: 22.3.2018.

Zníženie komplexnosti a nákladov na WAN

Podniky s pobočkami alebo vzdialenými miestami obvykle na účely smerovania a bezpečnosti využívajú mnohobodové produkty. Tieto produkty majú oddelené konzoly na správu, v dôsledku čoho sa správa stáva náročnou a dochádza aj k neúplnej viditeľnosti siete. Väčšina spoločností sa v súčasnosti usiluje o konsolidáciu týchto funkcionalít, aby sa znížila komplexnosť a zlepšila ich bezpečnostná pozícia a viditeľnosť. Spoločnosti chcú tiež na zníženie nákladov na WAN a zvýšenie dostupnosti nahradiť drahé MPLS spojeniami, ako sú napríklad internet a LTE. 70 % zákazníkov tvrdí, že ich súčasná WAN je slabá, pomalá, drahá a neúčinná na zavedenie cloudu.⁸

70%



zákazníkov tvrdí,
že ich súčasná
WAN je slabá,
pomalá, drahá
a neúčinná na
zavedenie cloudu.

Rastúca potreba účinnej ochrany pred hrozbami a kontroly SSL

Kybernetickí zločinci sa v rastúcej miere zameriavajú na nové paradigmy distribuovaných sietí. Napríklad v dôsledku priameho internetového prístupu k aplikáciám SaaS, obzvlášť v prípade, keď sú zariadenia mimo siete, sa zavedenie nových bezpečnostných stratégií určených pre distribuované podniky stáva vysoko kritickým faktorom. Z tohto dôvodu je na ochranu proti známym a neznámym hrozbám potrebná špičková funkcionalita ochrany proti hrozbám. Taktiež rastie objem zašifrovanej premávky (zašifrovaných je ~60 % celkovej premávky) spolu so škodlivým softvérom cieľným na SSL prenos.⁹ To znamená, že bude vysoký dopyt po kontrole SSL v reálnom čase, ktorá nebude spomaľovať premávku kritickú pre obchodné procesy.

Objem zašifrovanej premávky
v distribuovanej sieti

~60%

nárast
celkovej
premávky,
ktorá je
šifrovaná

spolu malvérom cieľným na SSL.

⁸ Andrew Lerner a Neil Rickard, "Trhová príručka pre infraštruktúru na okraji WAN siete", Gartner, 23.3.2017.

⁹ John Maddison, "Manažérsky pohľad: Trendy v oblasti hrozieb za r. 2017", Fortinet, 29. december 2017.

PRODUKTY SECURE SD-WAN



FortiGate

**FIREWALLY NOVEJ
GENERÁCIE (NGFW)
SD-WAN**

SD-WAN firewally značky FortiGate využívajú účelové bezpečnostné procesory, vďaka čomu poskytujú najlepšiu ochranu proti hrozbám dostupnú v odvetví a bránia pred väčšinou známych a neznámych pokročilých kybernetických útokov. Sú dostupné pre formát desktopového počítača a majú niekoľko variácií s integrovanými funkcionalitami PoE, 3G/4G, DSL a bezdrôtového pripojenia.



FortiOS

**SIETOVÝ OPERAČNÝ
SYSTÉM PRE
FORTIGATE (OS)**

FortiOS riadi všetky bezpečnostné a sieťové funkcie prostredníctvom jediného, intuitívneho operačného systému. Zlepšuje ochranu a viditeľnosť, pričom vďaka konsolidácii stoviek funkcií znižuje prevádzkové náklady a šetrí čas. Pomáha využívať rôzne funkcie SD-WAN, ako napríklad bezobslužná inštalácia, prioritizácia aplikácií s granulóznymi kontrolnými prvkami, upravovanie prevádzky s cieľom garantovať šírku pásma pre kritické aplikácie, kontrola SSL a jednodotková VPN na účely optimálneho využitia spoločného VPN prístupu do cloudu.



FortiGuard

**PREDPLATITEĽ-
SKÉ SLUŽBY
BEZPEČNOSTI**

Vývojový tím FortiGuard vyvíja účinné protiopatrenia na ochranu viac ako 310 000 zákazníkov spoločnosti Fortinet na celom svete. Poskytuje najčerstvejšie aktualizácie informácií o hrozbách pre služby ako napríklad IPS, AV, filtrovanie webu, botnet a sandboxing. Zákazníci si môžu zakúpiť predplatné pre jednotlivé služby alebo celé balíčky ako napríklad Enterprise, UTM a Threat Protection.

INÉ PRODUKTY



FortiManager

Centralizovaná správa
a jednotná politika



FortiCloud

Zero-touch deployment
pre FortiGate

PREČO SÚ RIEŠENIA FORTINET SECURE SD-WAN JEDINEČNÉ

Najlepšia bezpečnostná účinnosť v branži

Ochrana proti známym exploitom, škodlivému softvéru, aplikáciám a škodlivým webovým stránkam pomocou nepretržitého zberu a vyhodnocovania informácií o hrozbách poskytovaného službami bezpečnosti FortiGuard Labs. Ide o kritický faktor pre pobočky, ktoré umožňujú priamy internetový prístup pre aplikácie SaaS.

Databáza dynamických cloudových aplikácií (SaaS) a radič cesty WAN pre SD-WAN

FortiOS využíva viaceré interne vytvorené postupy, ktoré zabezpečujú viditeľnosť dovnútra tisícok aplikácií. V spojení s automatizovaným kontrolérom WAN pre SD-WAN to umožňuje najlepšiu úroveň služieb (SLA) pre aplikácie, ktoré sú kritické pre obchodné procesy.

Vysoký výkon IPsec VPN a kontroly SSL

Vďaka účelovým bezpečnostným procesorom poskytuje FortiGate najvyššiu priepustnosť (~10x vyššiu ako v prípade ostatných dodávateľov) v branži. Takisto podáva špičkový výkon a viditeľnosť v prípade zašifrovanej premávky. Fortinet je jedným z tých mála dodávateľov, ktorí udávajú výkon IPsec VPN a kontroly SSL pre každý podnikový firewall značky FortiGate.



KONKURENČNÉ POROVNANIE

	Fortinet	VeloCloud	Versa Networks	Cisco Viptela	Cisco Meraki
WAN Path Controller s aplikačnou SLA	✓	✓	✓	✓	častočne
NGFW s SSL inšpekciou	✓	✗	častočne	✗	častočne
Application Awareness	✓	✓	častočne	✓	častočne
Čas na dynamický failover	✓	✓	✓	✓	častočne
Scalable Auto IPsec VPN Overlays	✓	častočne	častočne	✓	častočne
Jedna konzola na správu bezpečnosti a SD-WAN	✓	✗	častočne	✗	✓
Bezdotyková konfigurácia	✓	✓	✓	častočne	✓
Celkové náklady spojené s vlastníctvom	✓	častočne	častočne	častočne	častočne

✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

Gartner 2017 Magic Quadrant for Enterprise Firewalls—“Leader”

V teste Gartner Magic Quadrant for Enterprise Firewalls urobil Fortinet výrazný posun z kategórie „Challenger Player“ do kategórie „Leader“. Jednou zo zahrnutých hlavných požiadaviek je škála produktu, ktorá musí podporovať rozšírené prostredie ako napríklad pobočku, kampus, dátovú centrálu a cloud.¹⁰



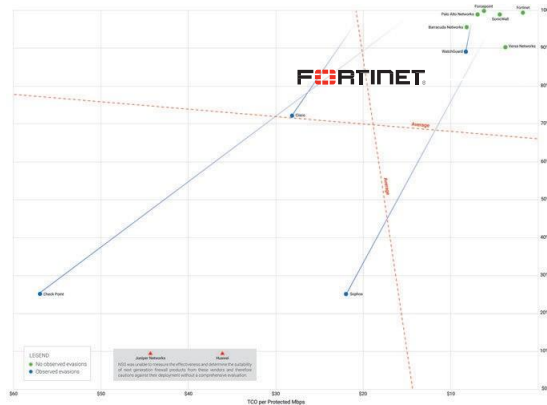
Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hills, Jeremy D'Hoinne, Rajpreet Kaur, July 10, 2017

Tento graf publikovala spoločnosť Gartner, Inc., v rámci váššieho výskumného materiálu. Preto by sa uvedený graf mal posudzovať v kontexte celého dokumentu. Dokument od spoločnosti Gartner poskytne spoločnosť Fortinet na požiadanie.

Spoločnosť Gartner neschvaľuje žiadneho dodávateľa, produkt ani službu uvádzanú vo svojich výskumných materiáloch a ani neodporúča používateľom technológiu, aby si vybrali iba tých dodávateľov, ktorí majú najvyššie hodnotenie či inú charakterizáciu. Výskumné materiály spoločnosti Gartner obsahujú iba názor výskumnej organizácie spoločnosti Gartner a nemajú sa chápať ako faktická skutočnosť. V súvislosti s uvedeným výkonom spoločnosť Gartner vylučuje všetky záruky, či už výslovné, alebo vyvoodené, vrátane akýchkoľvek záruk predajnosti či vhodnosti na určitý účel.

Testovanie firewallov novej generácie za rok 2018 od NSS Labs – „Odporúčané“

Vo výsledkoch testu firewallov novej generácie za rok 2018 od inštitúcie NSS Labs dostali produkty značky FortiGate odporúčanie za vynikajúci výkon a bezpečnosť.¹¹



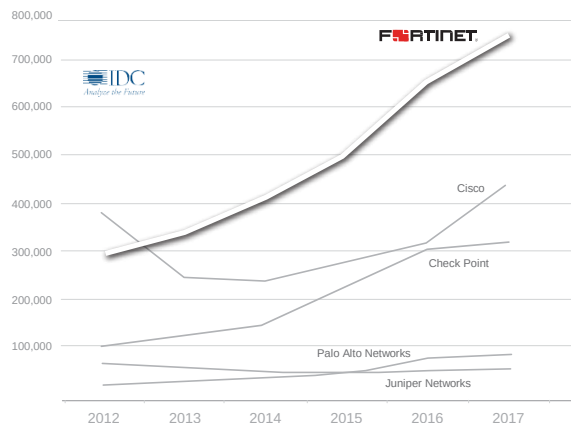
¹⁰ Adam Hills, Jeremy D'Hoinne a Rajpreet Kaur "Magický kvadrant firewallov podnikových sietí", Gartner, 10. júl 2017.

¹¹ "Bezpečnostná hodnotiacia mapa firewallov novej generácie (NGFW)", NSS Labs, júl 2018.

IDC Security Tracker – Najväčší trhový podiel v kategórii Distributed Enterprise

Podľa bezpečnostného rebríčka spoločnosti IDC sú FortiGate Enterprise Firewalls (rad 30 do 200) na prvom mieste na svete v trhovom podiele podľa počtu predaných kusov a obratu.

Podľa počtu dodaných kusov za rok (IDC)



zdroj: IDC Worldwide Security Appliances Tracker, apríl 2017 (podľa počtu dodaných kusov za rok)

HODNOTIACE OTÁZKY

- ☐ Rýchlo zavádzate cloudové aplikácie, ale máte problémy s reakčným časom?
- ☐ Zápasíte s rastúcim rozpočtom a komplexnosťou sietí WAN?
- ☐ Narážate na obmedzenia v šírke pásma, ktoré vplyvajú na vzdialené pobočky?
- ☐ Dokázate zabezpečiť priamy prístup na internet z pobočiek?
- ☐ Potrebujete povýšiť vašu infraštruktúru WAN na veľké distribuované nasadenie?
- ☐ Máte príliš veľa bodových produktov a snažíte sa znížiť komplexnosť?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Enterprise Firewall Solution
- NSE 3: FortiGate Entry Level

MULTICLOUDOVÁ BEZPEČNOSŤ

Organizácie rýchlo prechádzajú na viaceré cloudové inštalácie vrátane migrácie serverovej záťaže na verejné cloudy, ako napríklad Amazon Web Service alebo Microsoft Azure, alebo siahnu po aplikáciách SaaS. Zároveň väčšina podnikov v rámci procesu transformovania dátových centrál na privátne cloudy pokračuje v investovaní do virtualizačnej a softvérovo definovanej infraštruktúry. Multicloudové prostredie zahŕňajúce rozličné privátne a verejné cloudy sťažuje konsolidovanú bezpečnostnú prevenciu a detekciu.



Hlavnou IT prioritou v situácii, keď sú dáta uložené v IaaS alebo SaaS cloudoch, je zachovanie súkromia používateľov a dôvernosti dát. Z tohto dôvodu hrajú riešenia multicloudovej bezpečnosti kľúčovú úlohu pri ochrane privátnych, verejných a hybridných cloudov na zabezpečenie jednotnej bezpečnostnej pozície podnikových záťaží bez ohľadu na to, či sa prevádzkujú na fyzickej, virtuálnej alebo cloudovej infraštruktúre.

Riešenie Fortinet Multi-Cloud Security poskytuje kvalitnejšiu viditeľnosť, ochranu a kontrolu po celom rozšírenom priestore na útoky cloudu. Konceptia riešenia orientovaná na architektúru Security Fabric umožňuje viditeľnosť z jedného grafického užívateľského rozhrania a jednotnú bezpečnosť pre viaceré privátne cloudy, verejné cloudy a aplikácie SaaS.

Riešenie Fortinet Multi-Cloud Security tiež obsahuje konektory „Fabric Connectors“ do platforiem tretích strán vrátane služieb Amazon Web Services (AWS) a Microsoft Azure pre verejný cloud a VMware NSX a Cisco ACI pre softvérovo definované siete. Tieto konektory pomáhajú zaistiť dôslednú bezpečnosť naprieč prostrediami od viacerých dodávateľov tým, že umožňujú hlbokú, otvorenú integráciu naprieč bezpečnostným ekosystémom a automatizujú prevádzkové zmeny kritických komponentov.

TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Rýchly trhový rast v cloudovom priestore

Po zavedení infraštruktúry cloud computingu sa očakáva rýchly rast trhu cloudovej bezpečnosti. Inštitúcia IDC Research predpovedá, že výdavky na celosvetové služby verejného cloudu dosiahnu v roku 2018 sumu 160 miliárd dolárov¹² a že do roku 2020 bude viac ako 90 % podnikov využívať viaceré cloudové služby a platformy.¹³ Inštitúcia Gartner Research odhaduje, že bezpečnostné riešenia a riešenia na správu v súvislosti s IaaS a SaaS stúpnu v uvedenom období na 11 miliárd dolárov.¹⁴

Zvýšená prevádzka vnútri sietí

Ako sa budú miestne prostredia ďalej vyvíjať na privátne cloudy, toky sieťovej prevádzky sa budú postupne presúvať z tradičného smeru north-south na smer east-west. Do roku 2021 bude až 86 % celkovej prevádzky z dátových centrál v smere east-west namiesto smeru north-south.¹⁵ Náležitá kontrola všetkej prevádzky typu „east-west“ vykonávaná na účel zaistenia náležitej segmentácie záťaží poľahky rozšíri súčasný trh pre bezpečnosť dátových centrál v smere north-south až štvornásobne.

90%



podnikov bude do roku 2020 využívať viaceré cloudové služby a platformy.

86%



všetkej prevádzky z dátových centrál bude do roku 2021 v smere **east-west** namiesto smeru north-south.

¹² "Prognóza rastu výdavkov na služby verejného cloudu v tomto roku celosvetovo na 160 mld. USD," IDC, 18.1.2018.

¹³ "IDC FutureScape: Prognózy odvetvia IT celosvetovo na rok 2018," IDC, október 2017.

¹⁴ "Magický kvadrant pre firewally podnikových sietí," Gartner, 10.7.2017.

¹⁵ "Globálny cloudový index Cisco," Cisco, 1.2.2018.

PRODUKTY MULTICLOUDOVEJ BEZPEČNOSTI



FortiGate-VM

FortiGate-VM je ústredným prvkom cloudovej bezpečnosti. Ako virtuálna verzia našich ocenených fyzických zariadení FortiGate má FortiGate-VM rovnaké bezpečnostné a riadiace mikrogramové vybavenie FortiOS, ako aj funkcionality aktualizácie hrozieb FortiGuard.



FortiGate-VMX

Zosúladenie so softvérovo definovanými sieťami (SDN) ďalej zabezpečuje automatickú konfiguráciu a škálovanie kontroly siete. FortiGate-VMX je účelová verzia virtuálneho zariadenia FortiGate, ktorá poskytuje hĺbkovú integráciu dátovej a riadiacej vrstvy s VMware NSX, čím sa v prostrediach vSphere dosahuje pokročilá bezpečnosť a mikrosegmentácia.



Konektory FortiGate

Konektory „Fabric Connectors“ pre bezpečnostnú spleť umožňujú otvorenú integráciu architektúry Fortinet Security Fabric na účel automatizovaného vkladania firewallovej a sieťovej bezpečnosti v ekosystéme zákazníka do dynamických sieťových tokov s viacerými komponentmi. Do tejto kategórie patria popredné platformy SDN, ITSM a cloudu, ako napríklad Cisco, Vmware, Nuage, ServiceNow, AWS, Azure a Google, vo väčšej miere než akékoľvek iné riešenie dostupné v súčasnosti.

INÉ PRODUKTY

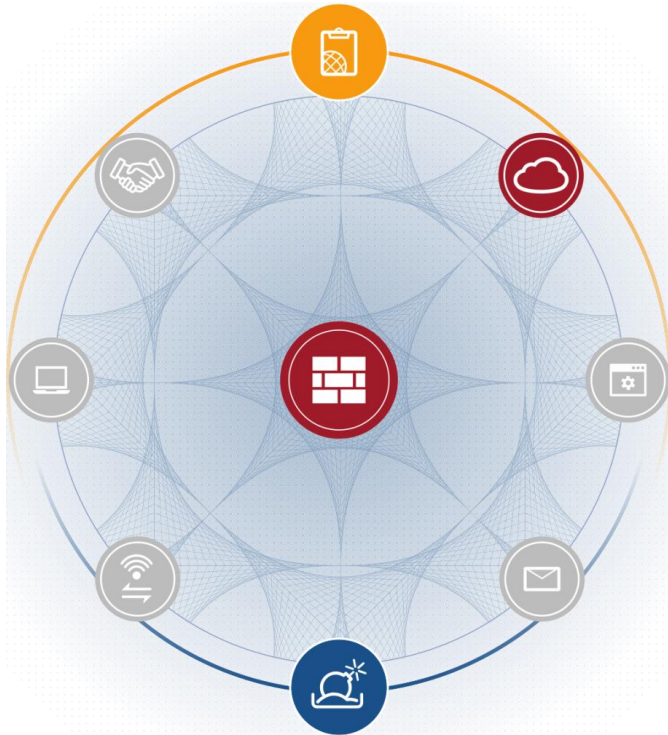


FortiCASB (cloud access security broker)
Táto služba poskytuje kritickú viditeľnosť používateľov a dát v cloudových aplikáciách.



Virtuálne zariadenia Fortinet
Široká škála sieťovej bezpečnosti pre privátne a verejné cloudy.

MULTICLOUDOVÁ BEZPEČNOSŤ FORTINET



Riešenie multicloudovej bezpečnosti umožňuje viditeľnosť z jedného grafického užívateľského rozhrania a jednotnú bezpečnosť pre viaceré privátne cloudy, verejné cloudy a aplikácie SaaS.

PREČO SÚ RIEŠENIA CLOUDOVEJ BEZPEČNOSTI FORTINET JEDINEČNÉ

Iba riešenia multicloudovej bezpečnosti Fortinet dokážu zvýšiť viditeľnosť a kontrolu nad celým privátnym, verejným a hybridným cloudovým prostredím organizácie s integráciou architektúry Fortinet Security Fabric.

Jednotná bezpečnostná pozícia naprieč privátnymi a verejnými cloudami

Fortinet umožňuje jednotnú aplikáciu bezpečných a predpisom zodpovedajúcich politík, ako aj viditeľnosti bezpečnostnej architektúry naprieč fyzickou, virtuálnou a cloudovou infraštruktúrou. Bezpečná konektivita siete „site-to-site“ VPN medzi miestnym a verejným cloudom zaisťuje bezpečnú aplikáciu a migráciu dát naprieč hybridným cloudom pri minimalizácii úniku dôverných údajov.

Segmentácia siete medzi koncovými bodmi v rámci cloudov a naprieč cloudami

Fortinet poskytuje mohutnú funkcionálnu kontrolu na kontrolovanie prevádzky „east-west“ v rámci privátnych a verejných cloudov, vďaka čomu sa znižuje koncentrácia rizika z hrozieb v silne konsolidovaných virtuálnych a cloudových prostrediach. Vnútrošnú segmentáciu a mikrosegmentáciu možno ľahko nasadiť do plochých, otvorených sietí bez prerušení, čím sa zabezpečí medzikoncová segmentácia s hladkými politikami založenými na používateľoch, aplikáciách a dátach.

Automatické škálovanie ochrany pre elastické cloudové záťaže

Keďže mnohé spoločnosti prechádzajú na využívanie cloud computing-u na elastické škálovanie webových a iných aplikácií, Fortinet zabezpečuje súkromie používateľov a utajenie dát v cloudovom meradle bez spomalenia práce. Firewallovú kontrolu možno zladit' do dynamických aplikácií a tokov softvérovo definovaných sietí, pričom kapacitu kontrolnej činnosti možno automaticky zväčšovať podľa rozsahu cloudových aplikácií. Prostredníctvom automatickej konfigurácie možno aplikovať príslušné bezpečnostné politiky pre nové a existujúce záťaže.



KONKURENČNÉ POROVNANIE

	Fortinet	Cisco	Check Point	Juniper	Palo Alto	Trend Micro
Podpora popredných verejných cloudov vrátane AWS a Azure	✓	✗	✓	✗	✓	✓
Podpora všetkých hlavných hypervízorových platforiem	✓	✓	✗	✗	✓	✗
Podpora kľúčových SDN platforiem vrátane NSX, ACI a OpenStack	✓	✗	✓	✗	✓	✗
Škálovateľný výkon a účinnosť virtuálnych zariadení	✓	✗	✓	✓	✗	✗
Široké spektrum ponúk virtualizovanej bezpečnosti	✓	✗	✓	✗	✗	✗
Gartner Enterprise Firewall MQ Leader	✓	✗	✓	✗	✓	✗

✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

NSS Labs and Gartner Magic Quadrant

Virtuálne zariadenia značky FortiGate tvoria súčasť triedy výrobkov, ktorých hardvér získal početné nezávislé hodnotenia a uznania vrátane hodnotenia „Odporúčané“ od NSS Labs a hodnotenia „Leader“ v Gartner Magic Quadrant for Enterprise Firewall.

Partnerská certifikácia

Integráciu a zosúladienie produktov FortiGate s poprednými privátnymi či verejnými cloudovými platformami certifikovali alebo uznali kľúčoví partneri vrátane hodnotenia vhodnosti VMware Ready for Networking and Security, VMware Ready for NFV, Cisco ACI, AWS Marketplace, Azure Marketplace, Azure Security Center a Google Cloud Platform.



Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hills, Jeremy D'Hoinne, Rajpreet Kaur, July 10, 2017

Tento graf publikovala spoločnosť Gartner, Inc., v rámci väčšieho výskumného materiálu. Preto by sa uvedený graf mal posudzovať v kontexte celého dokumentu. Dokument od spoločnosti Gartner poskytne spoločnosť Fortinet na požiadanie.

Spoločnosť Gartner neschvaľuje žiadneho dodávateľa, produkt ani službu uvádzanú vo svojich výskumných materiáloch a ani neodporúča používateľom technológie, aby si vybrali iba tých dodávateľov, ktorí majú najvyššie hodnotenie či inú charakteristiku. Výskumné materiály spoločnosti Gartner obsahujú iba názor výskumnej organizácie spoločnosti Gartner a nemajú sa chápať ako faktická skutočnosť. V súvislosti s uvedeným výskumom spoločnosť Gartner vylučuje všetky záruky, či už výslovné, alebo vyvodené, vrátane akýchkoľvek záruk predajnosti či vhodnosti na určitý účel.

HODNOTIACE OTÁZKY

- ☐ Využívala vaša organizácia v rámci projektov konsolidácie alebo transformácie dátovej centrál virtualizáciu, SND alebo iné technológie?
- ☐ Ako zabezpečujete viditeľnosť v zvýšenej prevádzke „east-west“ alebo prevádzke medzi virtuálnymi systémami?
- ☐ Nakoľko by bolo koncentrované vaše riziko, keby v silne konsolidovaných virtuálnych prostrediach došlo k narušeniu bezpečnosti?
- ☐ Využíva vaša organizácia verejné cloudy, ako napríklad AWS, Azure alebo Google?
- ☐ Akým spôsobom zabezpečujete, aby vaše aplikácie a dáta premigrované do cloudu mali rovnakú bezpečnostnú pozíciu, ako keby bežali vo vašej internej dátovej centrále?
- ☐ Migrujete aplikácie a dáta medzi miestnymi dátovými centrálnami/cloudami a verejným cloudom?
- ☐ Máte požiadavky týkajúce sa dôvernosti alebo dodržiavania predpisov, ktorými sa zabezpečuje, aby nedochádzalo k úniku dát z miestnych cloudov na verejné, a ako monitorujete únik dát a chránite sa pre ním?
- ☐ Ako zabezpečujete, aby k dátam v prostrediach SaaS, ako napríklad Office 365 alebo Salesforce.com, pristupovali iba oprávnení používatelia či zamestnanci?
- ☐ Ako zabezpečujete utajenie dát a dodržiavanie predpisov v súvislosti s dátami uloženými v aplikáciách SaaS, ako napríklad Office 365 alebo Salesforce.com?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Public Cloud Security

BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ

Podľa inštitúcie Verizon vyše 48 % narušení bezpečnosti dát v roku 2018 vzniklo priamym následkom hekerských útokov cielených na webové aplikácie.¹⁶ Webové aplikácie predstavujú pre hekerov atraktívny cieľ, lebo veľakrát ide o verejné aplikácie, ktoré vyžadujú otvorenosť voči internetu, aby stimulovali elektronické obchodovanie a biznis. Hlavným úložiskom citlivých informácií, ako napríklad čísla kreditných kariet, osobne identifikovateľné informácie (PII) a dôverné informácie, na ktoré sa vzťahuje duševné vlastníctvo, sú back-end databázy pripojené na webové aplikácie.



Odkedy sa obchod v rastúcej miere začal opierať o webové aplikácie, vydišerencovali sa webové aplikačné firewally (WAF) ako riešenia poskytujúce širokú škálu mechanizmov ochrany aplikačnej vrstvy, akými sú napríklad ochrana súborov „cookie“, skúšanie zhody protokolu HTTP, ochrana pred botmi a bezpečnostné pravidlá. Ich najvýznamnejšou vlastnosťou je však behaviorálna detekcia hrozieb. Dodávatelia WAF ju v súvislosti s ochranným mechanizmom proti zero-day útokmi a obchádzaniu podpisu uvádzajú ako najväčší rozdielový faktor voči riešeniam NGFW, IPS a riadiacej jednotky na doručovanie aplikácií (ADC). Nie však každý WAF ponúka organizáciám usilujúcim sa o bezpečnosť potrebnú funkcionality a škálu.

Riešenia bezpečnosti webových aplikácií Fortinet Web Application Security zahŕňajú WAF a ADC na ochranu aplikácií pred hrozbami, pričom zároveň poskytujú nástroje potrebné na plynulé škálovanie bezpečnostných aplikácií pre milióny používateľov. Naše robustné riešenie WAF (FortiWeb) vyniká v situáciách, kedy treba na riešenie zero-day útokov a známych zraniteľností použiť strojové učenie založené na umelej inteligencii (AI). To mu zároveň umožňuje takmer absolútne eliminovať falošné pozitívne signály, ktoré trápia iné riešenia WAF. Hladko sa integruje do architektúry Fortinet Security Fabric, aby tak umožnil obojsmerné zdieľanie informácií o hrozbách a automatizáciu bezpečnostných pracovných tokov a procesov.

¹⁶ „[Správa z prešetrovania narušení bezpečnosti dát z roku 2018](#)“, Verizon, 10.4.2018.

TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Produkty bezpečnosti webových aplikácií

Exploity v aplikáciách sú najčastejšou príčinou narušenia bezpečnosti

Inštitúcia Verizon uvádza, že zraniteľnosti webových aplikácií sú aj naďalej najvýznamnejším faktorom, ktorý prispieva k narušeniu bezpečnosti dát. Používanie odcudzených autentifikačných údajov sa stále drží na prvej priečke medzi hekerskými technikami narušenia bezpečnosti týkajúceho sa webových aplikácií.¹⁷



Inštitúcia Verizon uvádza, že **zraniteľnosti webových aplikácií** sú aj naďalej najvýznamnejším faktorom prispievajúcim k narušeniu bezpečnosti dát.

Rast šifrovanej prevádzky predbieha infraštruktúru

Len v 1. štvrťroku 2018 vzrástla šifrovaná prevádzka o 6 % oproti predchádzajúcemu štvrťroku.¹⁸ Hoci sa to príliš neuvádza, veľmi rýchlym tempom narastá zašifrovaná prevádzka webových aplikácií. Väčšina organizácií sa naháňa za šifrovaním svojich citlivých dát, aj keď tým preťažujú svoju existujúcu infraštruktúru na doručovanie aplikácií.



Len v 1. štvrťroku 2018 vzrástla **šifrovaná prevádzka o 6 %** oproti predchádzajúcemu štvrťroku.



FortiWeb

WEBOVÉ APLIKAČNÉ FIREWALLY (WAF)

Riešenie FortiWeb chráni hostované aplikácie pred útokmi, ktoré sa zameriavajú na známe a neznáme exploity. FortiWeb chráni aplikácie pred známymi zraniteľnosťami a zero-day útokmi prostredníctvom používania metód viacvrstvovej a korelovanej detekcie.



FortiADC

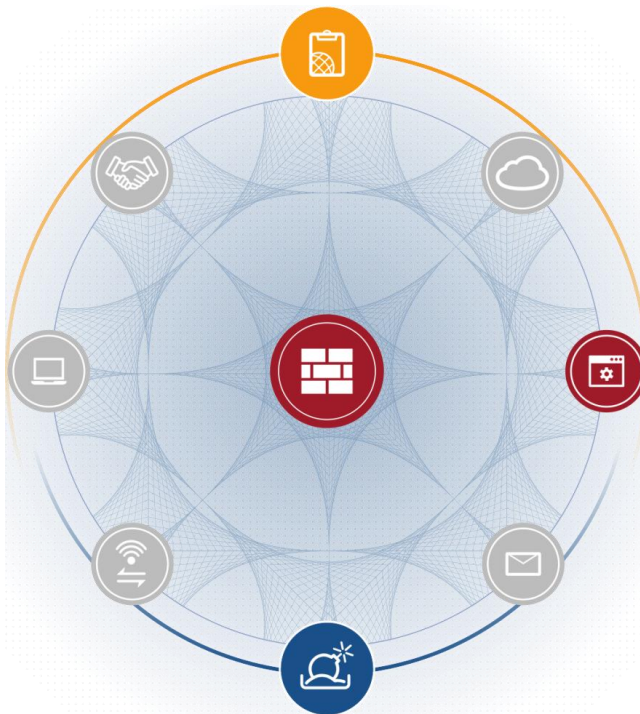
RIADIACE JEDNOTKY NA DORUČOVANIE APLIKÁCIÍ (ADC)

Riešenia ADC optimalizujú dostupnosť, používateľský zážitok, výkon a škálovateľnosť doručovania podnikových aplikácií. Trieda fyzických zariadení FortiADC poskytuje rýchle, bezpečné a inteligentné zrýchlenie a distribúciu náročných aplikácií v podniku.

¹⁷ "Správa z prešetrovania narušení bezpečnosti dát z roku 2018", Verizon, 10.4.2018.

¹⁸ "Správa o prostredí hrozieb z 1. štvrťroka 2018," Fortinet, máj 2018.

BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ FORTINET



Riešenie Web Application Security rozširuje architektúru Fortinet Security Fabric na obranu proti útokom cieľeným na slabé miesta vo webových aplikáciách.

PREČO SÚ RIEŠENIA BEZPEČNOSTI WEBOVÝCH APLIKÁCIÍ FORTINET JEDINEČNÉ

Úplné riešenie bezpečnosti webových aplikácií

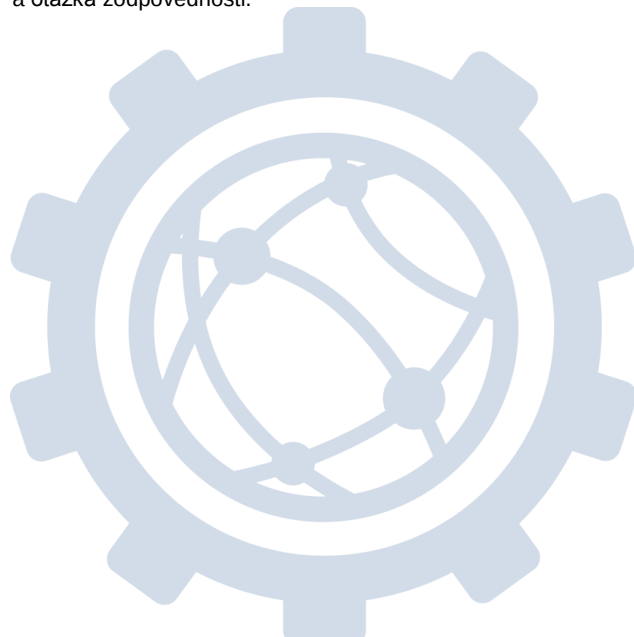
Iba Fortinet poskytuje úplné riešenie, ktoré pokrýva hlavné prvky bezpečnosti aplikácií. Toto riešenie obsahuje webové aplikačné firewally a radiace jednotky na doručovanie aplikácií. Taktiež zdokonaľujeme naše samoučiace sa systémy, aby sme lepšie skombinovali strojové učenie, hĺbkové učenie a AI algoritmy s globálnymi a lokálnymi informáciami o hrozbách v reálnom čase. Väčšina dodávateľov ponúka len bodové produkty, ktoré vyžadujú komplexné riešenie od viacerých dodávateľov náročné na inštaláciu a správu.

Integrácia do architektúry Fortinet Security Fabric

Naše portfólio bezpečnosti webových aplikácií je hlboko integrované do architektúry Fortinet Security Fabric. Prostredníctvom služieb FortiGuard Threat Intelligence spolu s antivírusovými, antimalvérovými signatúrami, signatúrami reputácie IP adries a útokov na aplikácie zabezpečujeme, aby boli aplikácie chránené pred najnovšími hrozbami. Kvôli ochrane proti pokročilým hrozbám je riešenie Web Application Security integrované do ďalších riešení ako napríklad firewally FortiGate, FortiMail a FortiSandbox. Takisto je integrované s riešeniami mnohých nezávislých dodávateľov – vrátane spoločností HP, IBM a Verisign.

Úplné, integrované riešenie

Riešenia Web Application Security od spoločnosti Fortinet sú optimalizované tak, aby v oblasti správy a zasielania správ dokázali pracovať spoločne s inými produktmi Fortinet. Všetky produkty majú podobné rozhranie, aby sa skrátil čas, ktorý tímy podpory potrebujú na zaučenie. Pri riadení menšieho počtu dodávateľov sa zjednodušuje modernizácia systému a otázka zodpovednosti.



	Fortinet	F5	A10	Imperva	Barracuda
Vysoké hodnotenie bezpečnosti z nezávislých zdrojov	✓	✓	✗	✓	✗
Úplné riešenie WAF a ADC	✓	✓	✓	✗ Iba WAF	✓
Súčasť širšieho integrovaného riešenia	✓	✗	✗	✗	✗
Dostupné v čínteľov faktorov	✓	✓	✓	✓	✓
Hodnotenie analytikov (WAF)	Gartner Challenger NSS Recommended	Gartner Leader NSS Recommended	Gartner Not rated NSS Not Rated	Gartner Leader NSS Not Rated	Gartner Challenger NSS Not Rated

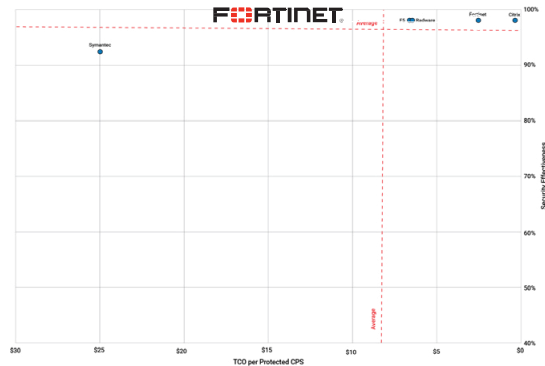
✓ = poskytovaná funkcionálna

✗ = nedostupná funkcionálna

NEZÁVISLÉ HODNOTENIE

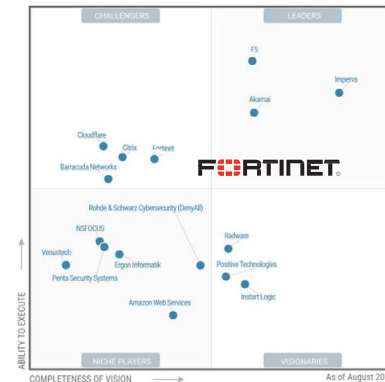
NSS Labs 2017 WAF Comparative Report and SVM – “Recommended”

Vo Web Application Firewall Comparative reporte and Security Value Map získal produkt FortiWeb hodnotenie „Recommended“. Produkt FortiWeb 3000E bol porovnávaný s piatimi konkurenčnými výrobkami, pričom sa v porovnaní s konkurenciou umiestnil celkovo veľmi dobre – prešiel všetkými testami a v oblasti bezpečnostná účinnosť spoločne obsadil prvé miesto, keď za celkovú hodnotu za rok 2017 získal hodnotenie „Nadpriemer“.



Gartner 2017 Magic Quadrant pre WAF – “Challenger”

V Gartner Magic Quadrant for Web Application Firewalls za rok 2017 od spoločnosti Gartner bol Fortinet druhýkrát po sebe vyhodnotený ako „Challenger“. Vďaka integrácii s architektúrou Fortinet Security Fabric, ako aj svojim neustálym technickým inováciám predstavuje FortiWeb bezproblémovú voľbu pre lídrov v oblasti bezpečnosti, ktorí hľadajú webový aplikačný firewall na ochranu svojich aplikácií orientovaných na web.



Magický kvadrant webových aplikačných firewallov od spoločnosti Gartner, 7.8.2017

Tento graf publikovala spoločnosť Gartner, Inc., v rámci väčšieho výskumného materiálu. Preto by sa uvedený graf mal posudzovať v kontexte celého dokumentu. Dokument od spoločnosti Gartner poskytne spoločnosť Fortinet na požiadanie.

Spoločnosť Gartner neschvaľuje žiadneho dodávateľa, produkt ani službu uvádzanú vo svojich výskumných materiáloch a ani neodporúča používateľom technológie, aby si vybrali iba tých dodávateľov, ktorí majú najvyššie hodnotenie či inú charakteristiku. Výskumné materiály spoločnosti Gartner obsahujú iba názor výskumnej organizácie spoločnosti Gartner a nemajú sa chápať ako faktická skutočnosť. V súvislosti s uvedeným výskumom spoločnosť Gartner vylučuje všetky záruky, či už výslovné, alebo vyvoodené, vrátane akýchkoľvek záruk predajnosti či vhodnosti na určitý účel.

HODNOTIACE OTÁZKY

- ☐ Ako v súčasnosti chránite svoje kritické webové aplikácie pred útokmi?
- ☐ Preverujete pravidelne bezpečnosť kódu – ak áno, ako často?
- ☐ Potrebujete spĺňať normy PCI DSS? Aké boli výsledky vášho posledného auditu PCI DSS?
- ☐ Obávate sa narušenia bezpečnosti citlivých údajov zákazníkov alebo vlastníckych informácií prostredníctvom vašich webových aplikácií?
- ☐ Prerastajú vaše bezpečné webové aplikácie kapacitu vášho aktuálneho zariadenia na vyrovnávanie záťaže serverov?
- ☐ Potrebujete na havarijnú obnovu aplikácií aplikácie, ktoré preklenujú viaceré dátové centrály?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Application Security
- NSE 3: Web Application Firewalls (FortiWeb)
- NSE 3: Application Delivery Controllers (FortiADC)

E-MAILOVÁ BEZPEČNOSŤ

E-mail je pre podniky kritickým nástrojom. Tiež však predstavuje prioritnú metódu doručovania ransomvéru, phishingu a útokov prostredníctvom firemných e-mailov (BEC). Analytici v odvetví varujú, že pokročilé hrozby poľahky obchádzajú tradičné mechanizmy ochrany založené na signatúrach či reputácii. Okrem toho odporúčajú vykonať opatrenia na obmedzenie nedostatkov vo funkcionalite obrany proti pokročilým hrozbám v aktuálnej vstupnej bráne na zabezpečenie e-mailu - secure email gateway (ak neprichádza do úvahy úplná výmena).



SEG je nainštalovaná medzi verejným internetom a firemným e-mailovým serverom a v konečnom dôsledku teda aj e-mailovou schránkou koncového používateľa. Je určená na blokovanie ransomvéru, phishingu a ďalších kybernetických hrozieb, ktoré sa pokúšajú o prienik do prichádzajúcich e-mailov, pričom zabezpečuje aj to, aby z odchádzajúcich správ podvodne neunikali citlivé údaje. Moderné riešenia SEG tiež pomáhajú zabezpečiť súlad s množstvom predpisov a firemných smerníc týkajúcich sa utajenia dát na účel ochrany duševného vlastníctva.

Riešenie e-mailovej bezpečnosti Fortinet Email Security sa opiera o vstupnú bránu na zabezpečenie e-mailu FortiMail, čím zabraňuje prieniku hrozieb až ku koncovému používateľovi, ochraňuje citlivé údaje pred náhodnou stratou a pomáha organizáciám spĺňať zákonné a firemné požiadavky. Riešenie FortiMail zabezpečuje v rámci architektúry Fortinet Security Fabric tento úsek širokého priestoru na digitálne útoky, pričom veľakrát využíva pokročilé služby a technológie bezpečnosti od FortiGuard Labs, ktoré zahŕňajú prevenciu vypuknutia nákazy, zablokovanie a rekonštrukciu obsahu, ochranu pri kliknutí na odkaz a analýzu krádeží identity. Fortinet Email Security v spojení s riešením FortiSandbox zabezpečuje nielen zablokovanie predtým neznámych e-mailových útokov, ale v rámci reakcie na celý životný cyklus útokov začínajúcich e-mailom aj aktualizáciu ochrany naprieč celou architektúrou Security Fabric.



TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

E-mail predstavuje v kybernetickej bezpečnosti riziko č. 1

Podľa Verizon Data Breach Investigations Report (DBIR) za rok 2018 od inštitúcie Verizon 49 % inštalovaného malvéru (nie z predajných miest) bolo nainštalovaných prostredníctvom škodlivého e-mailu.¹⁹ Viac ako 92 % malvéru a 96 % útokov sociálneho inžinierstva (napr. phishing) prichádza formou e-mailu.²⁰ E-mail taktiež predstavuje najbežnejšie miesto vstupu ransomvéru. Predpokladá sa, že celosvetové náklady vyplývajúce z útokov ransomvéru dosiahnu do roku 2019 hodnotu 11,5 mld. dolárov ročne.²¹

E-mailové útoky sú nákladné

Podľa FBI bolo v roku 2017 hlásených 15 690 prípadov útoku prostredníctvom firemného e-mailu a ich náklady spolu predstavovali odhadom 675 mil. dolárov, t.j. 52 000 dolárov na incident.²²

E-mailové útoky berú nielen peniaze

V marci 2018 americké ministerstvo spravodlivosti obvinilo istú organizáciu kybernetického zločinu z krádeže vyše 31 TB údajov a duševného vlastníctva z akademického prostredia, ktoré bolo obstarané a odcudzené v hodnote približne 3,4 mld. dolárov.²³



Viac ako **92 % malvéru** a **96 % útokov sociálneho inžinierstva** (napr. phishing) prichádza **formou e-mailu**.



V roku 2017 bolo hlásených **15 690** prípadov útoku prostredníctvom firemného e-mailu a ich náklady spolu predstavovali odhadom **675 mil. dolárov**, t.j. **52 000** dolárov na incident.



E-mailové útoky berú nielen peniaze.

¹⁹ Charlie Osborne, "Prudký nárast bezsúborových útokov v r. 2017, bezpečnostné riešenia ich nezastavujú," ZDNet, 15.11.2017.

²⁰ "Správa z prešetrovania narušení bezpečnosti dát z roku 2018", Verizon, 10.4.2018.

²¹ Steve Morgan, "Globálne škody z ransomvéru dosiahnu do roku 2019 odhadom sumu 11,5 mld. USD," Cybersecurity Ventures, 14.11.2017.

²² Kelly Jackson Higgins, "FBI: Ohlásené internetové zločiny prekročili v minulom roku sumu 1,4 mld. dolárov", Dark Reading, 9.5.2018.

²³ "Deväť íráncov obvinených z rozsiahlej kybernetickej krádeže podniknutej pre Islamské revolučné gardy", americké ministerstvo spravodlivosti, 23.3.2018.

PRODUKTY E-MAILOVEJ BEZPEČNOSTI



FortiMail

VSTUPNÁ BRÁNA NA ZABEZPEČENIE E-MAILU (SEG)

FortiMail je úplné riešenie dostupné v priestoroch spoločnosti ako fyzické alebo virtuálne zariadenie alebo ako hosťovaná služba spravovaná dodávateľom či ponuka v AWS/Microsoft Azure na požiadanie.

Poskytuje ochranu pred tradičnými a pokročilými e-mailovými útokmi, ktorá neustále dosahuje špičkové hodnotenie z nezávislých zdrojov, ako aj integrovaný súbor robustných prvkov ochrany dát vrátane funkcionality ochrany pred stratou dát, šifrovania založeného na identite a archivovania elektronickej pošty a mnohých ďalších.



FortiSandbox

DETEKCIA POKROČILÝCH HROZIEB

Riešenie FortiSandbox ponúka vysokoúčinnú kombináciu pokročilej detekcie, automatizovaného zmierňovania bez vplyvov, prenikavý prehľad a flexibilné nasadenie na zastavenie cielených útokov a následnej straty údajov. Taktiež predstavuje kľúčovú zložku nášho riešenia ochrany proti pokročilým hrozbám Advanced Threat Protection. Služba FortiSandbox Cloud Service je tiež dostupná so vstupnou bránou na zabezpečenie e-mailu FortiMail.

INÉ PRODUKTY



FortiAnalyzer

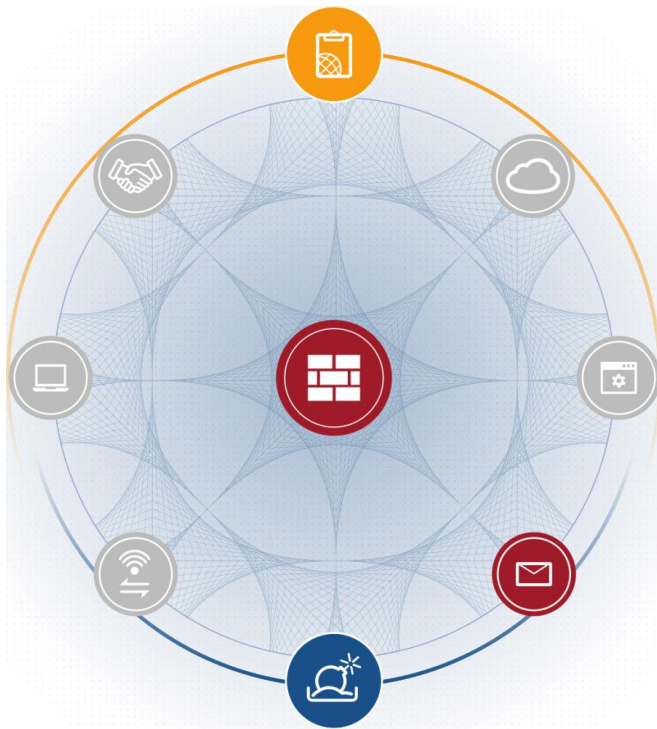
Ponúka kritický pohľad na hrozby a riziká a všade tam, kde sa vyžaduje okamžitá reakcia.



FortiSIEM

Správa sieťovej bezpečnosti, výkonu a zhody prostredníctvom jedného grafického užívateľského rozhrania.

E-MAILOVÁ BEZPEČNOSŤ FORTINET



Riešenie e-mailovej bezpečnosti sa integruje s architektúrou Fortinet Security Fabric, vďaka čomu sa dosahuje aktualizácia prvkov ochrany v odpovedi na úplný životný cyklus útokov začínajúcich e-mailom.

PREČO SÚ RIEŠENIA E-MAILOVEJ BEZPEČNOSTI FORTINET JEDINEČNÉ

Opakované špičkové hodnotenie od nezávislých organizácií

Pomocou nepretržitého zberu a vyhodnocovania informácií o hrozbách, ktorý zabezpečujú služby bezpečnosti FortiGuard Labs, chránia proti známym a neznámym hrozbám ako napríklad spam, malvér, ransomvér, spear phishing a útoky prostredníctvom firemných e-mailov.

Integrácia do architektúry Security Fabric

Okrem svojej výnimočnej účinnosti pri zastavovaní e-mailových útokov vďaka využívaniu riešenia FortiSandbox je Fortinet Email Security jedínnym riešením, ktoré automaticky odhaľuje a zdieľa informácie o celom životnom cykle e-mailových útokov v rámci architektúry Security Fabric. V tejto súvislosti sa treba zmieniť o natívnej integrácii a otvorených API, ktoré umožňujú zdieľanie s bezpečnostnými prvkami od spoločnosti Fortinet a od iných výrobcov naprieč celou organizáciou, a tak vám pomáhajú presunúť sa z permanentne reaktívnej na proaktívnejšiu bezpečnostnú pozíciu.

Najširšia škála tvarových faktorov

Kompletný súbor riešenia FortiMail a Email Security kompatibilného s bezpečnostnou sieťou je k dispozícii v podobe fyzických a virtuálnych zariadení vo variante pre cloudové služby spravované dodávateľmi a partnermi a dokonca aj pre viaceré verejné cloudy vrátane AWS a Azure. Nezáleží na tom, kde sa nachádza vaša e-mailová infraštruktúra, ani na tom, či si chcete bezpečnosť spravovať sami alebo sa obrátiť na profesionálneho partnera – FortiMail vždy dokáže splniť vaše potreby.

KONKURENČNÉ POROVNANIE

	Fortinet	Cisco	Proofpoint	Microsoft	Barracuda
ATD funkcionálna odporúčaná spol. Gartner	✓	✓	✓	✓	✓
Prvky integrovanej ochrany dát	✓	✓ Vysoký príplatok	✓ Vysoký príplatok	✓	✓
Vysoké hodnotenie bezpečnosti z nezávislých zdrojov	✓	✗	✗	✗	✗
Zdieľanie informácií na proaktívnu bezpečnosť	✓	✗ Nízka úroveň integrácie, >12 konzol	✗ Bodový produkt	✗ Bodové riešenie	✓ Len natívny e-mail a sieť
Činiteľ tvaru - v priestoroch spoločnosti, SaaS, verejný cloud	✓	✓ Bez možnosti verejného cloudu	✓ Bez možnosti verejného cloudu	✓ len SaaS	✓

✓ = poskytovaná funkcionálna

✗ = nedostupná funkcionálna

NEZÁVISLÉ HODNOTENIE

Virus Bulletin 2018 VBSpam+ certifikácia

Vstupná brána na zabezpečenie e-mailu FortiMail získala desiatykrát za sebou certifikát VBSpam+, pričom dva roky po sebe dostala najvyššie hodnotenie. FortiMail dokázal zachytiť 99,986 % všetkých spamov bez falošných pozitívnych výsledkov.²⁴



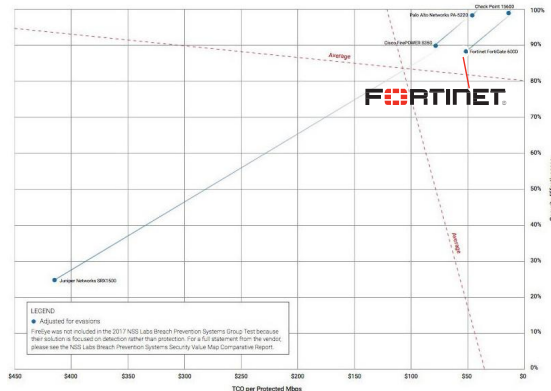
Certifikácia ICSA na obranu proti pokročilým e-mailovým hrozbám

Certifikácia spoločnosti ICSA Labs v 1. štvrtroku 2018 ukázala, že v rámci 1 224 testovacích behov certifikácie ATD-E-mail riešenie FortiMail odhalilo 99,8 % hrozieb škodlivých e-mailov pri šiestich falošných pozitívnych výsledkoch.²⁵



NSS Labs 2017 Breach Prevention System (BPS) – “Recommended”

V decembri 2017 NSS Lab predviedol nový test technológií BPS určený na hodnotenie schopnosti do 15 minút nielen detekovať, ale aj naozaj zabrániť neznámym (a menej známym) hrozbám. Bezpečnostná architektúra Fortinet Security Fabric (vrátane riešení FortiSandbox, FortiGate, FortiMail a FortiClient) získala vďaka svojej automatizovanej a vysoko granularnej detekcii, prevencii a odozve ďalšie hodnotenie „Odporúčané“. Fortinet preukázal mieru blokovania na úrovni 99,6 % s 0 falošnými pozitívnymi výsledkami, vynikajúci výkon a výborné TCO.²⁶



²⁴ Martijn Grooten a Ionuț Răileanu, „Porovnávacia správa VBSpam“, Virus Bulletin, jún 2017.

²⁵ „Správa z certifikačného testovania obrany pred pokročilými hrozbami za 1. štvrtrok 2018“, ICSA Labs, 2.4.2018.

²⁶ William Dean Freeman a Jessica Williams, „Správa z testovania systémov prevencie narušenia bezpečnosti“, NSS Labs, 13.12.2017.

HODNOTIACE OTÁZKY

- ☐ Čo by to znamenalo pre vašu organizáciu a váš tím, keby ste u vás mohli o polovicu zredukovať riziko ohrozenia kybernetickej bezpečnosti?
- ☐ Aké opatrenia ste zaviedli na boj s najnovšími pokročilými hrozbami? A čo v prípade ochrany proti útokom prostredníctvom firemných e-mailov?
- ☐ Aké sú vaše najdôležitejšie údaje a aké máte opatrenia na ich ochranu?
- ☐ Prešli ste na služby Microsoft Office 365 alebo Google G Suite?
- ☐ Unavuje vás, že pri svojom úsilí o zastavenie kybernetických hrozieb ste neustále v defenzíve? Aké prínosné by bolo, keby ste sa posunuli do proaktívnejšej bezpečnostnej pozície?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Email Security
- NSE 2: Advanced Threat Protection
- NSE 3: FortiMail
- NSE 3: FortiSandbox



OCHRANA PROTI POKROČILÝM HROZBÁM

Kybernetickí útočníci nejavia žiadne známky poľavenia. Preto nie je prekvapujúca skutočnosť, že podľa pozorovania FortiGuard Labs došlo v 1. štvrtroku 2018 k 27 % nárastu počtu jedinečných rodín malvéru a 35-násobnému rastu ransomvéru a že sa objavil nový globálny jav – neoprávnená ťažba kryptomeny (cryptojacking), ktorá v rovnakom období zaznamenala dvojciferný vzrast.²⁷



Túto situáciu ďalej zhoršujú dva nové inovačné prvky. Malvér ako služba (MaaS) je samoobslužný portál ponúkajúci nováčikom v oblasti kybernetických hrozieb na výber početné možnosti vrátane rodín malvéru, exploitov, C2 serverov a spambotov, aby mohli jednoducho len prostredníctvom pár kliknutí vytvoriť svoj útočný arzenál. Využívaním AI sa pracovnou rýchlosťou počítača generuje polymorfný malvér.

Na boj proti týmto prepracovaným hrozbám je potrebná technológia detekcie pokročilých hrozieb ako napríklad sandboxing. Sandboxy sú účelovo vytvorené na spúšťanie neznámych súborov v rámci diagnostického virtuálneho prostredia. Analyzujú správanie, aby mohli identifikovať nový malvér, na ktorý ešte neboli objavené signatúry. Kvôli dĺžke trvania analýzy sa však samotné sandboxy obvykle nasadzujú len na detekciu, pričom vyžadujú podniknutie odvetných krokov.

Spoločnosť Fortinet sa rozhodla pre iný prístup. Riešenie ochrany pred pokročilými hrozbami **Fortinet Advanced Threat Protection (ATP)** poskytuje sandboxing ako integrovanú funkciu zavedených bezpečnostných technológií, ktoré už fungujú v rámci bodov kontroly siete, e-mailu, webových aplikácií a koncových bodov. Týmto spôsobom sa zabezpečuje nielen to, že takmer všetok malvér je odvedený na kontrolu, ale že po jeho detekcii možno na účel automatizovanej odozvy a lepšej ochrany zdieľať nové informácie o neznámom malvére v rámci celej architektúry Security Fabric.

²⁷ Steve Morgan, [“5 najdôležitejších faktov, čísel a štatistík v oblasti kybernetickej bezpečnosti za rok 2018”](#), CSO, 23.1.2018.

TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Priemerná organizácia je už nabúraná

V minulom roku spoločnosť Fortinet vykonala takmer 3 000 hodnotení kybernetickej bezpečnosti, v ktorých počas 2 týždňov v každej spoločnosti pozorne monitorovala sieťovú prevádzku pomocou našich najnovších informácií o hrozbách. Pritom sme zistili, že priemerná organizácia bola narušená vyše štyrmi aktívnymi malvérmi alebo botmi.

V minulom roku stál ransomvér organizácie 5 mld. dolárov

Predpovedalo sa, že globálne škody z ransomvéru prekročia v roku 2017 sumu 5 mld. dolárov – pre porovnanie v roku 2015 to bolo len 325 mil. dolárov. To je 15-násobný vzostup len za obdobie dvoch rokov a budúcnosť bude ešte horšia. Predpokladá sa, že do roku 2019 škody stúpnu na 11,5 mld. dolárov, pričom sa očakáva, že každých 14 sekúnd padne za obeť ransomvéru jeden podnik.²⁷



Predpovedalo sa, že globálne škody z ransomvéru prekročia v roku 2017 sumu **5 mld. USD** – pre porovnanie v roku 2015 to bolo len 325 mil. USD.

²⁸ "Správa z prešetrovania narušení bezpečnosti dát z roku 2018", Verizon, 10.4.2018.

Malvér bol prítomný v 30 % prípadov narušenia

Podľa 2018 Verizon Data Breach Investigations Report od inštitúcie Verizon na 30 % z celkových 2 216 potvrdených prípadov narušenia bezpečnosti dát v minulom roku sa do určitej miery podieľal malvér.²⁸



30 % z celkových 2 216 potvrdených prípadov narušenia bezpečnosti dát v minulom roku sa od určitej miery opieralo o malvér.

Cloudová bezpečnosť – totálna fikcia

Odkedy organizácie ďalej pokračujú v úsilí o cloud ako súčasť svojich iniciatív digitálnej transformácie, dochádza k zaostávaniu v oblasti primeraných bezpečnostných opatrení v moderných sieťach. Mnohé spoločnosti sa naďalej opierajú o zastarané, tradičné bezpečnostné prvky zaradené priamo do sieťovej cesty. Predvídateľné organizácie s perspektívou do budúcnosti, ktoré prešli na technológie ATP nainštalované v priestoroch spoločnosti, s nedočkavosťou očakávajú rozšírenie alebo migráciu do verejného cloudu, aby získali rovnakú istotu ochrany voči dnešným sofistikovaným hrozbám.

Úsvit novej doby pre ťažbu kryptomeny

Začiatky malvéru na ťažbu kryptomeny siahajú do roku 2011, ale prudký vzostup sa zaznamenal až záverom roka 2017. V roku 2018 tento malvér naďalej rastie v dôsledku explózie kryptomenovej ekonomiky. Z tohto dôvodu sa na cryptojacking upriamili mnohí kybernetickí zločinci.

PRODUKTY ATP



FortiSandbox

DETEKCIA POKROČILÝCH HROZIEB

Riešenie FortiSandbox vo funkcii centrály informácií o útokoch zero-day prijíma a analyzuje nové súbory a URL odoslané bezpečnostnými prvkami organizácie zaradenými priamo do sieťovej cesty. Potom im priradzuje hrozbový rating a zdieľa lokálne informácie o hrozbách v reálnom čase s bezpečnostnou infraštruktúrou, čím sa zrychľuje odozva a zmierňovanie vplyvov predtým neznámych útokov.

INÉ PRODUKTY



FortiGate

NGFW ponúkajúce ochranu proti hrozbám s automatizovanou viditeľnosťou.



FortiProxy

Webová brána poskytujúca vysokoúčinnú kontrolu a zvýšenie bezpečnosti aplikácií.



FortiMail

Vysokoúčinná e-mailová bezpečnosť (fyzická alebo virtuálna).



FortiClient

Bezpečnosť koncových bodov, ktorá ponúka integrovanú viditeľnosť, riadenie a proaktívne obranné prvky.



FortiWeb

WAF, ktoré chráni hostované webové aplikácie pred známymi a neznámymi exploitmi.



FortiSIEM

Správa sieťovej bezpečnosti, výkonu a zhody prostredníctvom jedného grafického užívateľského rozhrania.



FortiADC

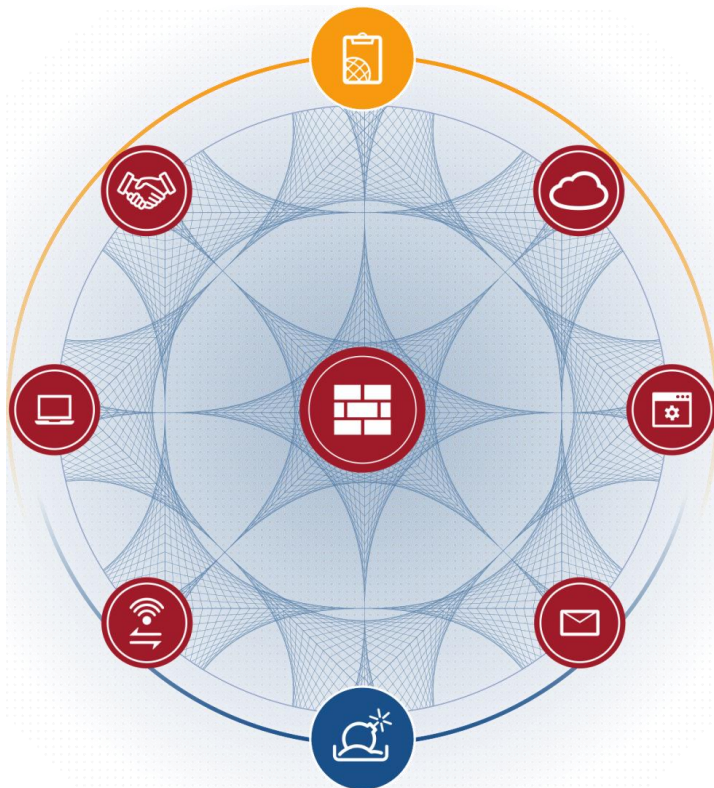
Poskytuje rýchle, bezpečné a inteligentné zrychlenie a distribúciu náročných aplikácií.



Partneri s API pripraveným pre bezpečnostnú sieť

Carbon Black, SentinelOne a Ziften sú natívne integrované s riešením FortiSandbox.

OCHRANA PROTI POKROČILÝM HROZBÁM FORTINET



Ochrana proti pokročilým hrozbám Fortinet integruje technológiu sandboxingu a iné funkcie detekcie na účel vytvorenia informácií v reálnom čase a aktualizovanej ochrany naprieč celou bezpečnostnou architektúrou Fortinet Security Fabric.

PREČO SÚ RIEŠENIA FORTINET ATP JEDINEČNÉ

Využitie architektúry Security Fabric na úplné pokrytie vektorov útoku na sieť, aplikácie a koncové body

Iba spoločnosť Fortinet poskytuje prvky, ktoré úplne pokrývajú primárne vektory útoku na sieť, aplikácie (e-mail a web) a koncové body. Je to možné preto, že sme vytvorili základy na automatické zdieľanie globálnych aj lokálnych informácií medzi jednotlivými zložkami systému, ktoré sú dostatočne silné na to, aby sa mohli nasaadiť kdekkoľvek v rámci organizácie. Fortinet je jediným dodávateľom, ktorý ponúka súčasť odporúčané NSS Labs pre firewally novej generácie, firewally dátových centrál, webové aplikačné firewally, pokročilú ochranu koncových bodov, detekciu prienikov a prevenciu prienikov.



Dostupné vo všetkých činiteľoch tvaru (vrátane verejného cloudu)

Zatiaľ čo niektorí dodávatelia ponúkajú prvky len ako fyzické zariadenia a iní zase len ako cloudové služby, Fortinet ponúka ochranu proti pokročilým hrozbám vo viacerých činiteľoch tvaru (v priestoroch spoločnosti, VM, hostovaná SaaS a verejný cloud).

Otvorená architektúra, ktorá obsahuje prvky nepochádzajúce od spoločnosti Fortinet

Našou nemennou koncepciou je, aby sme umožnili organizáciám nasadenie bezpečnostnej architektúry Fortinet Security Fabric a riešenia Advanced Threat Protection s prvkami od spoločnosti Fortinet, ako aj s prvkami od iných dodávateľov. Definované API umožňujú organizáciám integrovať do riešenia FortiSandbox jestvujúce sieťové prvky a prvky koncových bodov, aby sa tak dali odosielať objekty na analýzu, prijímať ratingy a absorbovať informácie o hrozbách. Náš program pripravenosti na bezpečnostnú spleť Fabric-Ready slúži na certifikáciu špecifických interakcií organizácie, ktoré využívajú uvedené API na zabezpečenie inštalácie zero-day.

KONKURENČNÉ POROVNANIE ATP

	Fortinet	FireEye	Palo Alto Networks	Cisco	Check Point	Trend Micro
Vysoké hodnotenie sandboxu z nezávislých zdrojov	✓	✗	✗	✓	✓	✓
Integrované riešenie						
Ent FW	✓	✗	✓	✓	✓	✓
SEG	✓	✓	✗	✓	✗	✓
WAF	✓	✗	✗	✗	✗	✗
EPP	✓	✗	✓	✗	✓	✓
Činitele tvaru						
Fyzický	✓	✓	✓	✓	✓	✓
Virtuálny	✓	✗	✗	✗	✗	✓
SaaS	✓	✓	✓	✓	✓	✗
Otvorené API	✓	✗	✗	✗	✗	✗

✓ = poskytovaná funkcionálnosť

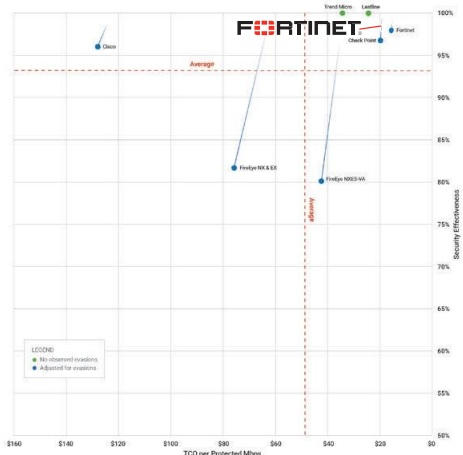
✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

Riešenie Fortinet Advanced Threat Protection je v súčasnosti jediným dostupným riešením, ktoré získalo odporúčanie od NSS Labs a certifikáciu ICSA pre sieťovú, e-mailovú a webovú aplikačnú bezpečnosť a bezpečnosť koncových bodov.

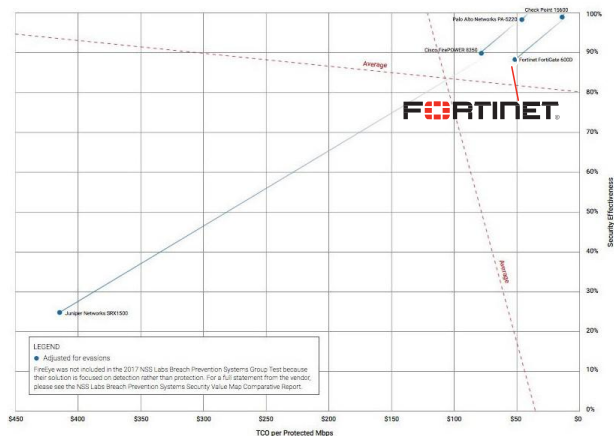
NSS Labs 2017 Breach Detection Systems (BDS) Test Report – “Recommended”

Riešenie Fortinet Advanced Threat Protection získalo v teste Breach Detection Systems za rok 2017 NSS Labs štvrtýkrát za sebou hodnotenie „Odporúčané“. Riešenia FortiSandbox a FortiClient (ATP Agent) dosiahli rating detekcie narušenia bezpečnosti 99,0 %. Ďalšími kritériami v teste boli bezpečnostná účinnosť, miera detekcie malvéru a únikov, výkonnosť a celkové náklady vlastníctva.²⁹



NSS Labs 2017 Breach Prevention Systems (BPS) Test Report – “Recommended”

Riešenie Advanced Threat Protection bolo od NSS Labs ocenené hodnotením „Odporúčané“, keď dosiahlo mieru blokovania narušení 99,6 % a mieru detekcie falošných pozitívnych signálov 0,00 %.³⁰

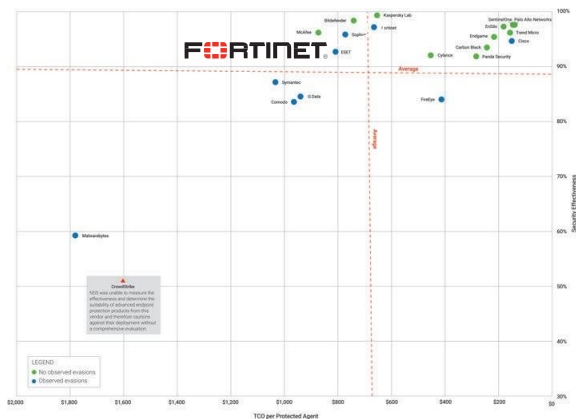


²⁹ Dipti Ghimire a James Hasty, “[Správa z testovania systémov detekcie narušenia bezpečnosti](#)”, NSS Labs, 19.10.2017.

³⁰ William Dean Freeman a Jessica Williams, “[Správa z testovania systémov prevencie narušenia bezpečnosti](#)”, NSS Labs, 13.12.2017.

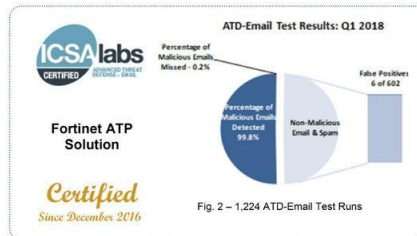
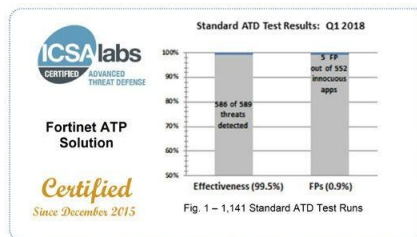
NSS Labs 2018 Advanced Endpoint Protection (AEP) Test—“Recommended”

Skupinový test AEP od NSS Labs hodnotí produkty na bezpečnostnú účinnosť, výkonnosť a TCO. Riešenie FortiClient s integrovaným riešením FortiSandbox získalo hodnotenie „Odporúčané“ pri priemernej bezpečnostnej účinnosti vyše 97,3 %, nulových falošných pozitívnych signáloch a nízkych TCO.³¹



Certifikácie ICSA 2017 Advanced Threat Defense

Od decembra 2015 je riešenie Fortinet Advanced Threat Protection (vrátane riešení FortiGate, FortiMail, FortiClient a FortiSandbox) nepretržitým držiteľom certifikácie Štandard obrany proti pokročilým hrozbám ICSA (pre sieť) a neskôr ICSA ATD-Email.³²



³¹ Rabin Bhattarai, Edsel Valle, Morgan Dhanraj a Ryan Kelly, „[Správa z testovania pokročilej ochrany koncových bodov](#)“, NSS Labs, 17.4.2018.

³² „[Správa z certifikačného testovania obrany proti pokročilým hrozbám za 1. štvrťrok 2018](#)“, ICSA Labs, 2.4.2018.

HODNOTIACE OTÁZKY

- ☐ Na aké údaje, duševné vlastníctvo a komunikáciu sa vzťahujú predpisy o utajení, bezpečnosti či iné regulačné rámce? Aké informácie sú vzhľadom na úspešnosť vášho podnikania najkritickejšie (a najviac strážené)?
- ☐ Zažili ste už nejaké incidenty s ransomvérom alebo neoprávnenou ťažbou kryptomeny (alebo ste počuli o vašich partneroch či kolegoch, ktorí ich zažili)? Ak áno, aké opatrenia máte zavedené na zníženie rizika, ktorému je vaša organizácia vystavená?
- ☐ Koľko potenciálnych bezpečnostných incidentov sa u vás vyšetruje každý štvrtrok?
- ☐ Koľko z týchto incidentov sa začalo e-mailom? Koľko z nich bolo stiahnutých z webu? Koľké boli stiahnuté, kým bol zamestnanec pripojený na podnikovú sieť, resp. kým bol z nej odpojený?
- ☐ Máte skúsenosť s narušenou webovou stránkou alebo webovou aplikáciou (alebo ste počuli o partneroch či kolegoch, ktorí majú takúto skúsenosť)?
- ☐ Plánujete prejsť na cloud, práve naň prechádzate alebo ste už naň prešli? Aké sú vaše starosti ohľadom zabezpečenia aplikácií, údajov a služieb v cloud e proti súčasným hrozbám kybernetickej bezpečnosti?

NSE TRÉNINGOVÉ MODULY

- NSE 2: The Fortinet Security Fabric (includes ATP)
- NSE 3: FortiMail
- NSE 3: FortiWeb
- NSE 3: FortiClient
- NSE 3: FortiSandbox

BEZPEČNÝ JEDNOTNÝ PRÍSTUP

Pre mnohých sú ústredným bodom pri zabezpečovaní siete externé hrozby prichádzajúce z internetu. Ale vzhľadom na existenciu mobilnej pracovnej sily, koncepciu BYOD („prines si svoje vlastné zariadenie“) a rozmach IoT zariadení bez obrazového výstupu stúpajú hrozby z vektorov interného útoku. Z tohto dôvodu sa tiež zvyšuje význam zabezpečenia interného prístupu.



Na ochranu siete proti interným útokom je potrebné vedieť, čo sa na vašej sieti nachádza, a byť schopný riadiť, kam uvedené zariadenia prístupujú. Je nutné identifikovať a izolovať zabezpečené prenosné počítače, ktoré sa vracajú do siete s vírusom. Nové senzory IoT využívajúce sieť by mali mať prístup iba k tým aktívam, ktoré sú potrebné pre ich rolu. Moderné siete vyžadujú nepretržité skenovanie zariadení na sieti a uplatňovanie prístupových politík pri vstupovaní do každého miesta na sieti.

Riešenie bezpečného jednotného prístupu **Fortinet Secure Unified Access** ponúka komplexnú bezpečnosť pre infraštruktúru LAN a poskytuje najpružnejšiu bezpečnostnú platformu s presadzovaním bezpečnostnej politiky v celom priestore medzi koncovými bodmi. Úzko integruje riadenia **FortiGate** a riešenie **Network Access Control** v jadre siete, zariadenia **FortiSwitch** a bezdrôtové prístupové body **FortiAP**, aby tak umožnilo spoločnú bezpečnostnú politiku, ktorá rozširuje firewallovú ochranu až na okraj siete.

TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Power-over-Ethernet

Čím ďalej, tým viac zariadení pripájajúcich sa na drôtové porty z nich čerpá nielen internetovú konektivitu, ale aj elektrinu. Pôvodne technológiu napájania cez ethernet (PoE) využívali len bezdrôtové AP, ale v súčasnosti sa o funkcionality napájania cez drôtové pripojenie opiera stále viac zariadení a senzorov podporujúcich IoT. PoE switch porty sa nasadzujú v čoraz väčšom počte pri videokamerách, správe budov a osvetľovaní.

Posun z normy 802.11n na normu 802.11ac Wave 2

Bezdrôtová konektivita zostáva základnou požiadavkou väčšiny spoločností. Rastúca rýchlosť a lepšia spoľahlivosť vychádzajúca z novších noriem spôsobili postupné vylepšovanie prístupových bodov na Wi-Fi. Spoločnosti v súčasnosti pri plánovaní bezdrôtových sietí vyvažujú náklady prístupových bodov s vyššou priepustnosťou cenovo prístupnejšími možnosťami.

Rozmach zariadení IoT

S prudkým vzostupom IoT zariadení v podnikových sieťach nebola odpoveď na otázku, čo sa nachádza v sieti, nikdy ťažšia či dôležitejšia. IoT zariadenia sú prirodzene nezabezpečené, preto je potrebná ich identifikácia a segmentácia, aby nedochádzalo k infekcii v smere east-west.



Rast PoE
z IoT

Bezdrôtová konektivita
zostáva základnou
požiadavkou väčši-
ny spoločností.



Prudký nárast zariadení IoT

PRODUKTY BEZPEČNÉHO JEDNOTNÉHO PRÍSTUPU



FortiAP

INTEGROVANÉ BEZDRÔTOVÉ RIEŠENIE

Rad FortiAP rozširuje bezpečnostné politiky FortiGate až po bezdrôtovú sieť. Prístupové body FortiAP riadené radičom WLAN zabudovanom do riešenia FortiGate zabezpečujú viditeľnosť a správu prostredníctvom známeho GUI. Sú ideálne pre centrály, pobočky a vzdialené pobočky a obsahujú aj variant pre vonkajšie prostredie.



FortiSwitch

DRÔTOVÉ RIEŠENIE

Prepínače bezpečného prístupu FortiSwitch sú funkčne bohaté, ale nákladovo efektívne, pričom odrážajú potreby veľkých firemných kampusov alebo menších firemných pobočiek. Modely s vysokou hustotou portov (24 a 28 portov) a podporou normy 802.11at PoE dokážu napájať všetko od prístupových bodov cez VoIP telefóny až po dohľadacie kamery.



Sieťový prístup Fortinet

RIEŠENIE RIADENIA PRÍSTUPU DO SIETE (NAC)

Riešenie NAC od Fortinetu využíva na presnú profiláciu každého zariadenia, ktoré sa pripája do siete, početné zdroje informácií. Zariadeniu sa po pripojení prideli prístup k aktívam a informáciám primeraným pre daný druh zariadenia. Riešenie NAC je škálovateľné na nasadenia po celom svete a tiež podporuje rôznorodý ekosystém dodávateľa.

INÉ PRODUKTY



FortiAuthenticator

Centralizované riadenie používateľských identít, ktoré zjednodušuje správu.



FortiToken

Rad tokenových riešení, ktorý poskytuje silnú autentifikáciu pre bezpečný prístup a transakcie.



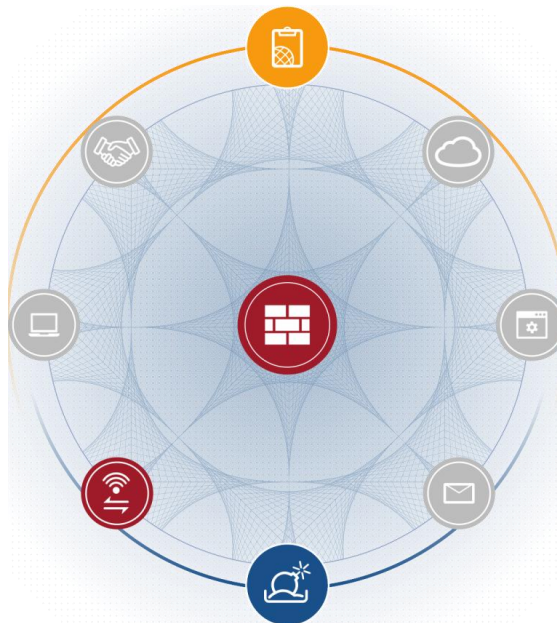
FortiExtender/ FortiExtender Cloud

Prostredníctvom celúlnej infraštruktúry LTE poskytuje WAN pripojenie k firewallu na zabezpečenie spoľahlivosti, resp. zvýšenej priepustnosti.



FortiPresence Spája WiFi lokalizáciu a analýzu s cieľom pochopiť výskyt a správanie.

BEZPEČNÝ JEDNOTNÝ PRÍSTUP FORTINET



Riešenie The Secure Unified Access sa integruje do architektúry Fortinet Security Fabric a komplexnej ochrany LAN infraštruktúry.

PREČO SÚRIEŠENIA THE SECURE UNIFIED ACCESS OD FORTINET JEDINEČNÉ

Vyváženie prístupu, výkonu a ochrany bez negatívnych vplyvov

Podniky v súčasnosti požadujú rýchly, transparentný prístup ku kritickým aplikáciám a dátam, a to z ktoréhokoľvek miesta a z množstva zariadení, nad ktorými už správcovia nemajú plnú kontrolu.

Riešenie bezpečného jednotného prístupu Fortinet Secure Unified Access poskytuje pevne integrovanú infraštruktúru – prístup, práca v sieti a bezpečnosť, ktorá dokáže splniť tieto požiadavky bez negatívneho ovplyvnenia výkonu či bezpečnosti.

Podpora komplexnej bezpečnosti naprieč infraštruktúrou

Riešenie Fortinet-u Secure Unified Access v prvom rade dokonale dopĺňa podnikov architektúru, pričom rozširuje bezpečnostnú architektúru Fortinet Security Fabric od jadra až po okraj. Zjednocuje aj rôzne prvky riešenia, čím poskytuje spoločný prínos väčší ako súčet jednotlivých jeho častí. Spoločný operačný systém pre celú sieť poskytuje lepšiu viditeľnosť a kontrolu nad prevádzkou v sieti, ako aj zjednodušené riadenie. Fortinet ďalej ponúka tri možnosti inštalácie zohľadňujúce rozmanité požiadavky podnikov na WLAN v súčasnosti.



KONKURENČNÉ POROVNANIE

Vlastnosť	Fortinet	Cisco	HP/Aruba	Aerohive	Ruckus/ARRIS
Enterprise WLAN	✓	✓	✓	✓	✓
UTM v Access Point	✓	✗	✗	✗	✗
Enterprise switching	✓	✓	✓	✓	✓
Firewall novej generácie	✓	✓	✗	✗	✗
Single-Pane-of-Glass manažment	✓	✗	✗	✗	✗
NAC	✓	✓	✓	✗	✗
Gartner MQ WLAN/LAN	✓	✓	✓	✓	✓
Integrovaná podniková bezpečnosť-LAN-WAN	✓	✗	✗	✗	✗

✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

Gartner 2018 Magic Quadrant for LAN/WLAN – “Niche”

V 2018 Gartner Magic Quadrant pre infraštruktúru drôtového a bezdrôtového LAN prístupu za rok 2018 od spoločnosti Gartner bola spoločnosť Fortinet uvedená ako poskytovateľ riešení drôtovej a bezdrôtovej infraštruktúry podnikovej kategórie.



Magic Quadrant for the Wired and Wireless LAN Access Infrastructure, Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint, July 2018

Tento graf publikovala spoločnosť Gartner, Inc., v rámci väčšieho výskumného materiálu. Preto by sa uvedený graf mal posudzovať v kontexte celého dokumentu. Dokument od spoločnosti Gartner poskytne spoločnosť Fortinet na požiadanie. Spoločnosť Gartner neschvaľuje žiadneho dodávateľa, produkt ani službu uvádzanú vo svojich výskumných materiáloch a ani neodporúča používať žiadnu technológiu, aby si vyberali iba dodávateľov s najvyšším hodnotením. Výskumné materiály spoločnosti Gartner obsahujú iba názor výskumnej organizácie spoločnosti Gartner a nemajú sa chápať ako faktická skutočnosť. V súvislosti s uvedeným výskumom spoločnosť Gartner vylučuje všetky záruky, či už výslovné, alebo vyvoodené, vrátane akýchkoľvek záruk predajnosti či vhodnosti na určitý účel.

HODNOTIACE OTÁZKY

- ☐ Okrem prvkov prístupovej vrstvy sa usilujete aj o bezpečnosť?
- ☐ Predstavuje zjednodušené riadenie kľúčový prvok?
- ☐ Už máte FortiGate?
- ☐ Máte veľa malých miest (rozptýlená maloobchodná štruktúra)?
- ☐ Potrebujete bezpečnosť na okraji pre malú pobočku?
- ☐ Máte veľké verejné priestory s úspornou RF funkcionalitou?
- ☐ Máte malý personál a potrebujete riešenie, ktoré sa ľahko inštaluje a riadi?
- ☐ Robíte si starosti, aby ste vedeli, aké IoT zariadenia sú na vašej sieti?

NSE TRÉNINGOVÉ MODULY

- NSE 3: Wireless Infrastructure Products
- NSE 3: Wireless Integrated Products
- NSE 3: FortiSwitch
- NSE 3: FortiAuthenticator

BEZPEČNOSŤ KONCOVÝCH BODOV

Zariadenia koncového bodu predstavujú pre organizácie jeden z najbežnejších vektorov útoku a prieniku. Podľa jednej štúdie až 63 % organizácií nedokáže monitorovať zariadenia koncového bodu, keď tieto opustia podnikovú sieť, pričom v 53 % prípadov počet koncových bodov infikovaných malvárom za posledných 12 mesiacov stúpol.³³ Podľa inštitútu SANS sa 74 % hrozieb dostalo do organizácií vo forme prílohy elektronickej pošty alebo odkazu.³⁴ A podľa inštitúcie Verizon v 30 % prípadov narušenia bezpečnosti išlo o malvér nainštalovaný na koncových bodoch.³⁵

Uvedené čísla týkajúce sa koncových bodov možno čiastočne pripísať prudkému vzrastu mobility, zvýšenej autonómii koncových používateľov a väčšiemu prístupu do cloudu. Koncové počítače nie sú vždy za firemným firewallom, čím sa vlastne tieto zariadenia dostávajú na okraj siete. Koncové body musia byť schopné obrany proti hrozbám; ak infikované zariadenie kontaminuje širšiu internú sieť, následné škody môžu mať pre podnik ničivé následky.



Zároveň sa neustále zvyšuje agresivnosť hrozieb. Modely MaaS v súčasnosti nielenže pomáhajú automatizovať útoky, ale aj objemovo a rýchlostne znásobujú hrozby.

Navyše býva bezpečnosť koncových bodov uzatvorená vo svojom vlastnom izolovanom priestore. Nedostatočná integrácia medzi riešeniami koncových bodov a riešeniami sieťovej bezpečnosti spomaľuje odozvu na hrozby. Preto sa môže malvér potichu šíriť prostredím – laterálnym pohybom infikovať viaceré zariadenia alebo vyhľadávať cenné ciele na účel exploatacie.

Riešenie bezpečnosti koncových bodov **Fortinet Endpoint Security** integruje bezpečnosť koncových bodov so sieťovou bezpečnosťou vrátane riešení FortiClient a FortiSandbox pracujúcich s produktmi FortiGate a FortiAnalyzer. Naše riešenie bezpečnosti koncových bodov poskytuje viditeľnosť založenú na riziku, riadenie súladu, správu zraniteľností a automatizáciu. Proaktívne chráni koncové body pomocou technológie rozpoznávania malvéru na základe vzorov, ochrany proti exploitom na základe správania, filtrovania webu a aplikačného firewallu. Natívne sa integruje s riešením FortiSandbox a ponúka zabudovaného VPN agenta na bezpečný vzdialený prístup.

³³ "Náklady nezabezpečených koncových bodov", Ponemon Institute, jún 2017.

³⁴ Lee Neely, "Prehľad o prostredí hrozieb z roku 2017", SANS Institute, august 2017.

³⁵ "Správa z prešetrovania narušení bezpečnosti dát z roku 2018", Verizon, 10.4.2018.

TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Podľa spoločnosti IDC sa do roku 2020 očakáva, že celosvetový trh firemnej bezpečnosti koncových bodov prekročí sumu 5 mld. dolárov.³⁶ Pozoruje sa opätovný záujem o integráciu bezpečnosti koncových bodov a sieťovej bezpečnosti na preklenutie bezpečnostnej medzery a potreby automatizovanej reakcie na hrozby.

Obmedzená viditeľnosť, súlad a riadenie koncových bodov

Koncové body už nie sú jednotným rozšírením firemného IT. Ako dôkaz, že sa už nachádzajú mimo dosahu IT, 56 % opýtaných profesionálov z oblasti IT uvádza, že nedokážu stanoviť súlad zariadení koncového bodu, pričom 70 % udáva „podpriemernú“ schopnosť minimalizovať škody vzniknuté zlyhaním koncového bodu.³⁷

Rýchlo sa vyvíjajúce prostredie hrozieb preniká k zraniteľným koncovým bodom

Podľa spoločnosti Gartner „Do roku 2021 bude pokračovať trend, že 99 % využitých zraniteľností už bolo profesionálom v oblasti bezpečnosti a IT známych najmenej 1 rok.“³⁸ Udržiavanie hygieny koncových bodov je čím ďalej, tým náročnejšie. V dôsledku rozdelenia funkcií tímy pre sieťovú bezpečnosť obvykle nemajú ani veľkú kontrolu nad záplatovaním a majú len malú kontrolu nad voľnosťou konania pri koncovom používaní. Zároveň sa však IT musí konfrontovať s únikmi z narušených koncových bodov.

³⁶ [Trhová prognóza IDC: Celosvetová prognóza bezpečnosti koncových bodov, 2016–2020](#), IDC, október 2016.

³⁷ ["Náklady nezabezpečených koncových bodov"](#), Ponemon Institute, jún 2017.

³⁸ Greg Young, Ako reagovať na prostredie hrozieb v roku 2018, Gartner, 28.11.2017.

Moderné, rýchlo sa pohybujúce útoky vyžadujú automatizovanú reakciu

Aby sa moderné útoky vyhýbali detekcii a mohli infikovať systémy, využívajú nové distribučné kanály, ako napríklad sociálne inžinierstvo, a nasadzujú nové techniky, akými sú viacstupňové a bezsúborové útoky. K narušeniu môže dôjsť v priebehu niekoľkých minút alebo len sekúnd.

Na účinnú detekciu a obranu proti týmto útokom je potrebné koordinovať a automatizovať bezpečnosť. Integrované riešenie sieťovej bezpečnosti dokáže poskytnúť optiku koncových bodov nad rámec základného zdieľania informácií o hrozbách, pričom súčasne umožňuje automatizovanú reakciu na potenciálne hrozby. Preto možno útoky a incidenty identifikovať a izolovať v reálnom čase.

Do roku 2021 bude

99%



využitých zraniteľností známych profesionálom v oblasti bezpečnosti a IT najmenej 1 rok.

Produkty bezpečnosti koncových bodov



FortiClient

**BEZPEČNOSŤ
KONCOVÝCH
BODOV**

Riešenie FortiClient posilňuje bezpečnostnú pozíciu podniku vďaka zlepšenej viditeľnosti koncových bodov, riadeniu súladu, proaktívnym prvkom obrany a automatizácii. Fabric Agent odosiela do bezpečnostnej siete telemetrické údaje koncového bodu vrátane informácií o zariadeniach, ID používateľov, zraniteľností a rizikových skóre.

FortiClient proaktívne chráni koncové body proti najnovším sofistikovaným hrozbám prostredníctvom integrácie antimalvéru, ochrany proti exploitom, filtrovania webu, obranných prvkov aplikačného firewallu a sandboxu. Na potlačenie hrozieb a reguláciu vypuknutia nákazy umožňuje automatizáciu založenú na politike a tiež obsahuje zabudovanú VPN na bezpečný vzdialený prístup.



FortiSandbox

**DETEKCIA
POKROČILÝCH
HROZIEB**

FortiSandbox analyzuje nové súbory a URL, s ktorými organizácia prišla do styku, automaticky im prideluje hrozbový rating a dynamicky generuje lokálne informácie o hrozbách špecifické pre danú organizáciu, vďaka čomu sa urýchľuje odozva a zmierňujú sa vplyvy predtým neznámych útokov.

Iné produkty



FortiGate

NGFW ponúkajúce ochranu proti hrozbám s automatizovanou viditeľnosťou.



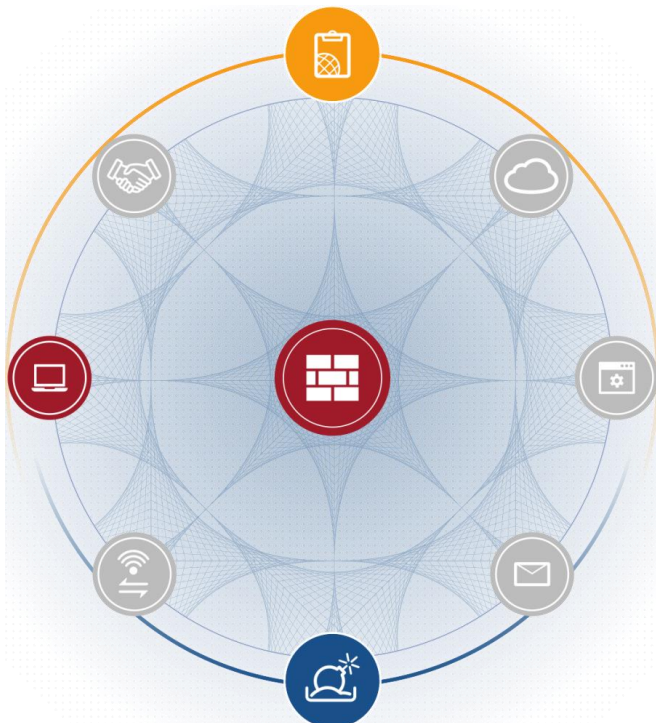
FortiAnalyzer

Ponúka kritický pohľad na hrozby a riziká a všade tam, kde sa vyžaduje okamžitá reakcia.



FortiClient je kompatibilný s AV a EDR riešeniami **prípravenými pre bezpečnostnú sieť.**

BEZPEČNOSŤ KONCOVÝCH BODOV FORTINET



Riešenie bezpečnosti koncových bodov po integrácii s architektúrou Fortinet Security Fabric poskytuje poznatky v reálnom čase, na základe ktorých sa dá konať, a automatizuje reakciu na hrozby pri útokoch využívajúcich exploitu a pri pokročilom malváre.

PREČO SÚ RIEŠENIA BEZPEČNOSTI KONCOVÝCH BODOV FORTINET JEDINEČNÉ

Viditeľnosť a riadenie koncových bodov založené na riziku

Riešenie Fortinet Endpoint Security umožňuje organizáciám viditeľnosť a riadenie založené na riziku naprieč všetkými koncovými bodmi na identifikáciu zraniteľností a prioritizáciu záplatovania koncových bodov, ako aj využívanie automatizácie založenej na politike na účel potlačenia hrozieb a regulácie vypuknutia náказы. Viditeľnosť koncových bodov, ktoré sú v sieti a mimo siete, v reálnom čase umožňuje uplatňovanie politík a kontrolných prvkov pre všetky koncové body. Takisto zabezpečuje automatickú detekciu zraniteľností koncových bodov a pružné záplatovanie.

Integrácia do architektúry Fortinet Security Fabric

Riešenie Fortinet Endpoint Security je integrované s technológiou sandboxingu na automatickú detekciu a blokovanie neznámych hrozieb. Zdieľa informácie o hrozbách z jednotlivých koncových bodov naprieč všetkými koncovými bodmi a bezpečnostnými prvkami v rámci prepojenej bezpečnostnej architektúry Security Fabric. Takisto sa môže integrovať s antivírusovými riešeniami a riešeniami detekcie a odozvy v koncových bodoch od iných poskytovateľov bez toho, aby tým dochádzalo k vzniku konfliktov.

KONKURENČNÉ POROVNANIE

Vlastnosť	Fortinet	Palo Alto Networks	Cisco	Sophos
Zdieľanie telemetrických údajov z koncových bodov s firewallom	✓	✗	✓	častočne
Audit bezpečnosti so skórovaním rizika	✓	✗	✗	✗
Softvérová inventarizácia	✓	✗	✗	✗
Presadzovanie súladu koncových bodov	✓	Je potrebný samostatný agent globálnej ochrany	Je potrebný samostatný nástroj NAC (ISE)	✗
Skenovanie zraniteľnosti koncových bodov so záplatovaním	✓	✗	✓	✗
Zdieľanie informácií o hrozbách naprieč podnikom	✓	obmedzené	✓	✗
Karanténa koncových bodov	✓	Je potrebný samostatný agent globálnej ochrany	Je potrebný samostatný nástroj NAC (ISE)	✗
Integrovaný sandbox	✓	✓	častočne	✗
Integruje sa so širokou škálou sieťovej infraštruktúry, firewallmi, AP, prepínačmi	✓	len firewall	✗	✗
Jediný agent pre VPN, telemetriu, SSO a EPP	✓	✗	✗	✗
Kompatibilita s tradičným EPP a AV novej generácie	✓	rôzne – môže dochádzať ku konfliktom	✓	rôzne

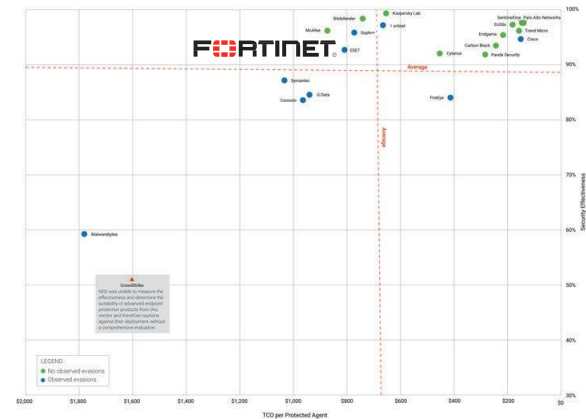
✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

NEZÁVISLÉ HODNOTENIE

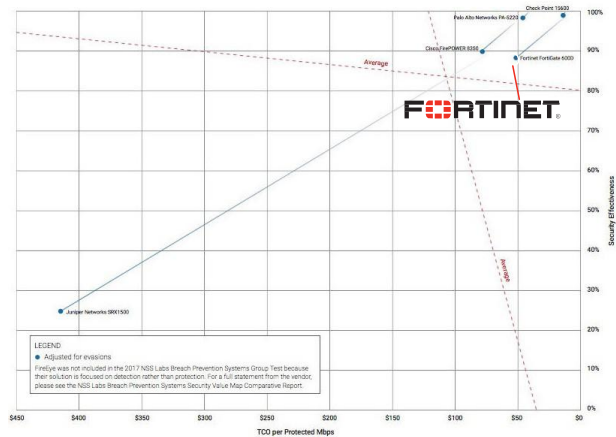
NSS Labs 2018 Advanced Endpoint Protection (AEP) Test—“Recommended”

Riešenie FortiClient s integrovaným riešením FortiSandbox získalo hodnotenie „Odporúčané“ pri priemernej bezpečnostnej účinnosti vyše 99,3 %, zero false pozitívnych signáloch a nízkych TCO.³⁹



NSS Labs 2017 Breach Prevention Systems (BPS) Test Report—“Recommended”

Produkty Fortinet boli od NSS Labs ocenené hodnotením „Odporúčané“, keď dosiahli mieru blokovania narušení 99,6 % a mieru detekcie falošných pozitívnych signálov 0,00 %.⁴⁰



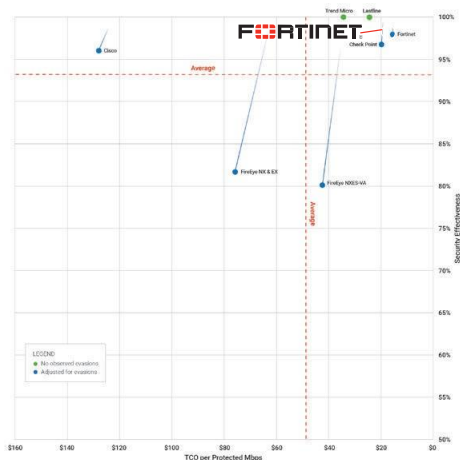
³⁹ Rabin Bhattarai, Edsel Valle, Morgan Dhanraj a Ryan Kelly, “[Správa z testovania pokročilej ochrany koncových bodov](#)”, NSS Labs, 17.4.2018.

⁴⁰ William Dean Freeman a Jessica Williams, “[Správa z testovania systémov prevencie narušenia bezpečnosti](#)”, NSS Labs, 13.12.2017.

NEZÁVISLÉ HODNOTENIE

NSS Labs 2017 Breach Detection Systems (BDS) Test Report—"Recommended"

Produkty Fortinet dosiahli hodnotenie „Odporúčané“ s ratingom detekcie narušenia bezpečnosti 99,0 %. Ďalšími kritériami v teste boli bezpečnostná účinnosť, miera detekcie malvéru a únikov, výkonnosť a celkové náklady vlastníctva.⁴¹



HODNOTIACE OTÁZKY

- ☐ Je u vás v súčasnosti viditeľnosť všetkých nasadených zariadení koncového bodu naprieč celou organizáciou – vrátane mobilných zariadení BYOD a produktov IoT?
- ☐ Akú mieru kontroly má správa IT nad nasadenými zariadeniami koncového bodu? Do akej miery jednotliví používatelia riadia, resp. spravujú prenosné počítače a ostatné prenosné zariadenia, čo sa týka aplikácií a updateov?
- ☐ Ako sa v súčasnosti chránite proti dnešným e-mailovým útokom?
- ☐ Aké ďalšie obranné prvky okrem lokálne nainštalovaného AV máte zavedené na ochranu koncových bodov pred pokročilými e-mailovými exploitmi, akými sú napríklad bezsúborové útoky?
- ☐ Obávate sa narušenia bezpečnosti citlivých údajov zákazníkov alebo vlastníckych informácií prostredníctvom malvérových útokov?
- ☐ Obávate sa, že vypuknutie nákazy ransomvérom môže prerušiť vašu činnosť, prípadne že náprava môže vašu organizáciu stať čas a peniaze?

NSE TRÉNINGOVÉ MODULY

- NSE 2: Endpoint Security
- NSE 3: FortiClient
- NSE 3: FortiSandbox

⁴¹ Dipti Ghimire a James Hasty, "Správa z testovania systémov detekcie narušenia bezpečnosti", NSS Labs, 19.10.2017.

SPRÁVA A ANALÝZA

Organizácie majú obvykle network operations centrá a security operations centrá vyčlenené buď ako osobitné organizácie, alebo osobitné funkcie. V oboch prípadoch nebývajú NOC a SOC integrované a nezdediať si informácie. Tým sa spomaľuje identifikácia útokov a narušení a obzvlášť sa brzdí schopnosť organizácie reagovať a nakoniec v prípade potreby vykonať nápravu.

Riešenia správy a analýzy Fortinet Management and Analytics pokrývajú riadenie IT ako aj bezpečnostných rizík naprieč celým podnikom. Zatiaľ čo bezpečnostné produkty Fortinet sú už unifikované s našou bezpečnostnou architektúrou Security Fabric prostredníctvom zdieľania informácií, riešenia správy a analýzy pomáhajú organizovať a koordinovať bezpečnostnú činnosť vrátane zahrňovania informácií z bezpečnostných prvkov mimo skupiny produktov značky Fortinet. Riešenie Management and Analytics viac ako iné riešenia Fortinet búra bariéry medzi NOC a SOC, pričom poskytuje komplexný a adaptívny pohľad na celú sieť, aby bolo možné rýchlo identifikovať hrozby a reagovať na ne. Toto riešenie taktiež pomáha riadiť súlad a dostupnosť aplikácií, čím do veľkej miery redukuje komplexnosť bezpečnostných operácií.



TRHOVÁ DYNAMIKA A HYBNÉ FAKTORY

Izolované riešenia môžu spôsobiť nezistené narušenie

Vedúce organizácie v odvetví na celom svete a zo všetkých obchodných vertikál zostávajú v rastúcom počte obeťami sieťových narušení bezpečnosti. Podľa inštitúcie Verizon celkový počet potvrdených narušení bezpečnosti údajov stúpol v roku 2017 z 1 935 na 2 216.⁴² Vzrastajúca úspešnosť útokov je sčasti spôsobená množstvom bodových riešení (v priemere 30 rôznych dodávateľských riešení) nasadených v NOC a SOC, ktoré preťažujú personál nekorelovanými a neprioritizovanými informáciami, pričom potenciálne hrozby nechávajú nespozorované, kým nie je neskoro. Detekcia narušení stále trvá stovky dní, k čomu treba pripočítať ďalšie dni strávené izolovaním a nápravou.

Nedostatok kvalifikovaného personálu v oblasti kybernetickej bezpečnosti

Organizácie sú do budúcnosti vystavené rastúcej potrebe skúseného personálu v oblasti kybernetickej bezpečnosti, ale nachádzajú neustále sa zmenšujúcu globálnu ponuku potrebných zdrojov. Najnovšie správy uvádzajú, že v celosvetovom meradle je neobsadených vyše 1 milióna voľných pracovných miest. Mnohé organizácie sa buď usilujú o outsourcing NOC a SOC, alebo vyhľadávajú lepšie riešenia, ktoré dokážu udržať krok s neustále sa vyvíjajúcim prostredím hrozieb.

⁴² "Správa z prešetrovania narušení bezpečnosti dát z roku 2018", Verizon, 10.4.2018.

PRODUKTY SPRÁVY A ANALÝZY



FortiAnalyzer

FortiAnalyzer zhromažďuje, analyzuje a koreluje údaje z produktov Fortinet na účel zabezpečenia zvýšenej viditeľnosti a robustných bezpečnostných výstražných informácií. V spojení so službou indikátorov narušenia FortiGuard Indicators of Compromise (IOC) tiež poskytuje prioritizovaný zoznam narušených hostiteľov, čím umožňuje vykonanie rýchleho zásahu.



FortiCloud

FortiCloud je cloudová služba na zasielanie hlásení a správ určená pre produkty sieťovej bezpečnosti Fortinet a produkty jednotného prístupu Fortinet. Poskytuje zjednodušenú metódu na nasadenie, správu a zasielanie hlásení o uvedených produktoch bez pokročilých funkcií riešení FortiAnalyzer alebo FortiManager.



FortiManager

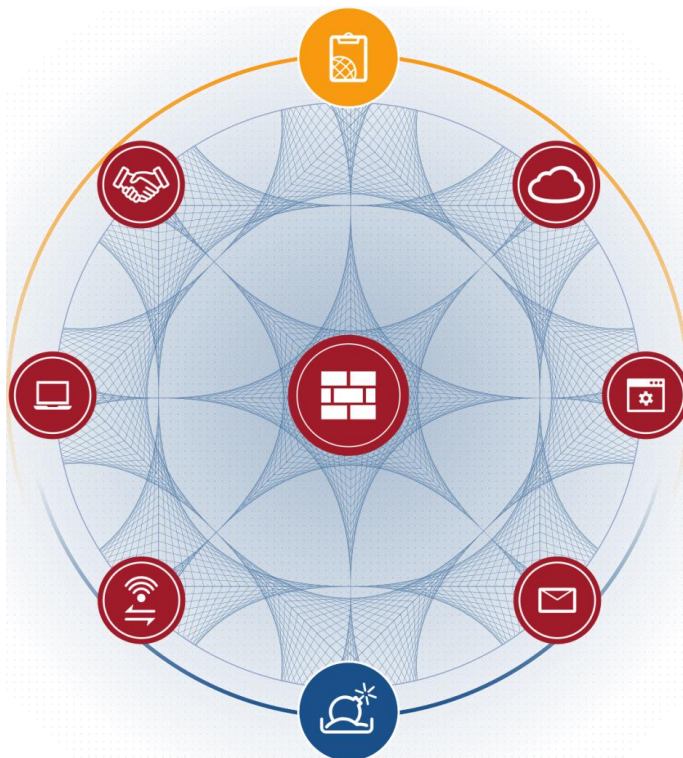
FortiManager poskytuje single-pane-of-glass manažment v rámci rozšíreného podniku za účelom získania poznatkov z celosieťovej prevádzky a hrozieb a tiež na účel správy politik. Obsahuje funkcie na potlačenie hrozieb aj špičkovú funkcionalitu škálovateľnosti, ktorá umožňuje správu až 10 000 zariadení Fortinet.



FortiSIEM

FortiSIEM poskytuje patentovanú analýzu umožňujúcu konanie, ktorá vzájomne koreluje údaje z NOC a SOC. Pomocou vlastnej identifikácie prvkov pripojených do siete pevne riadi sieťovú bezpečnosť, výkon a súlad, ako aj adaptívnu kontrolu nad prevádzkou v sieti, pričom využíva jediné grafické užívateľské rozhranie.

SPRÁVA A ANALÝZA FORTINET



Riešenie správy a analýzy umožňujú účinnú správu, viditeľnosť a získavanie poznatkov z celej bezpečnostnej architektúry Fortinet Security Fabric

PREČO SÚ RIEŠENIA SPRÁVY A ANALÝZY FORTINET JEDINEČNÉ

Zjednodušená bezpečnostná konfigurácia

Ak centralizujete a automatizujete inštalácie a konfiguračné úlohy, potom dochádza k tomu, že dochádza k opakovaniu úloh v určenom čase. To znamená, že sa strávi menej času inštaláciou a vzniká menej ľudských chýb. Keď však uvážite, aký široký dosah má architektúra Fortinet Security Fabric, tento prínos sa ešte znásobí, nakoľko konfiguračne presahuje tradičné hranice produktov. Vďaka tejto šírke architektúry Security Fabric je prínos (a riziko problémov bez tohto riešenia) v rovnako veľkom rozsahu. Celé je to potom o zjednodušení bezpečnostnej konfigurácie, aby sa znížil inštalačný čas a zmenšil počet ľudských chýb. Hlavnou zložkou v tomto prípade je FortiManager – jedna konzola pre celú architektúru Security Fabric.

Jeden bod kontroly

Na to, aby sme odhalili súčasné prepracované útoky, opierame sa o dáta z viac sieťových prvkov než kedykoľvek predtým. Tieto dáta navyše nám poskytujú perspektívy, ktoré sú potrebné na zablokovanie útokov. Nanešťastie, rýchlosť dát, ktoré treba kontrolovať, je ochromujúca, najmä v súvislosti s tým, že si bezpečnostní analytici uvedomujú, že na získanie potrebných perspektív musia siahnúť po viacerých nástrojoch, resp. konzolách. Aj keď bezpečnostný nástroj poskytujúci jedinú perspektívu môže odhaliť problémy, ktoré treba riešiť, chýba mu širší kontext, a tiež nebude vedieť správne prioritizovať kroky. Na druhej strane riešenia správy a analýzy Fortinet zbierajú obrovský objem telemetrických údajov v rámci celej bezpečnostnej architektúry Security Fabric a analyzujú ich cez jeden bod kontroly. Keďže všetko sa analyzuje cez jeden kontrolný prvok, je ľahké identifikovať najdôležitejšie priority.

Analýza NOC-SOC

Moderné siete sú komplexné a dynamické, pričom jednotlivé prvky sa pripájajú na sieť a odpájajú z nej podľa ľubovôle – a to všetko pri rozdielnej úrovni zraniteľnosti a bezpečnostnej ochrany. Táto prevádzková perspektíva priestoru na útoky, ako aj skutočnosť, že tento priestor je v neustálom pohybe, sa pri bezpečnostných vyšetrovaniach zriedkakedy berie do úvahy. Namiesto toho sa prešetrovatelia opierajú o statický (a preto nepresný) pohľad na priestor na útoky. To znamená, že rozsah objavených bezpečnostných skutočností je obvykle neúplný. Budú chýbať prvky, ktoré sa práve pripojili na sieť, a dôjde k mrhaniu zdrojov na ochranu či opravu prvkov, ktoré už dávno zo siete odišli.

NOC-SOC analýza značí, že bezpečnostné poznatky v reálnom čase sa porovnávajú s prevádzkovým pohľadom na priestor na útoky v reálnom čase. Ak sa výkonové problémy vychádzajúce z NOC zahrnú do prešetrovaní podnietených zo SOC, dôjde k presnému nastaveniu rozsahu a k použitiu zdrojov tam, kde je to účinné, a často aj k objaveniu nových bezpečnostných poznatkov. Spojením NOC a SOC sa zlepšuje bezpečnostná účinnosť.

KONKURENČNÉ POROVNANIE

	Fortinet	Palo Alto	Check Point	Cisco	Splunk	LogRhythm	IBM
Single-pane-of-glass menežment & reporting	✓	✓	✗	✗	✗	✗	✗
Správa firewallov a sieťových prvkov	✓	✓	✓	✓	✗	✗	✗
SIEM	✓	✗	✗	✗	✓	✓	✓
Pracovné toky NOC-SOC	✓	✗	✗	✗	✗	✗	✗
Bezpečnostný rating a pridelenie skóre	✓	✗	✗	✗	✗	✗	✗
Automatizácia medzi izolovanými oblasťami	✓	✗	✗	✗	častočne	častočne	častočne
CMDB	✓	častočne	častočne	častočne	✗	✗	✗
UEBA	✓	✗	✗	✗	✓	✓	✓

✓ = poskytovaná funkcionálnosť

✗ = nedostupná funkcionálnosť

HODNOTIACE OTÁZKY

- ☐ Zažili ste v minulom roku narušenie bezpečnosti? Ak áno, aký bol jeho dosah a ako sa pociťoval?
- ☐ Koľko riešení dodávateľov bezpečnostných produktov momentálne používate, aby ste obstáli pri narušení bezpečnosti?
- ☐ Ako si vaše NOC a SOC zdieľajú v súčasnosti dáta?

NSE TRÉNINGOVÉ MODULY

- NSE 2: The Fortinet Security Fabric (vr. Management & Analytics)
- NSE 3: FortiAnalyzer
- NSE 3: FortiManager
- NSE 3: FortiCloud
- NSE 3: FortiSIEM

SLUŽBY

FortiGuard

Výskumní pracovníci FortiGuard neustále prečesávajú kybernetický priestor, aby odkrývali nové hrozby a vyvíjali účinné protiopatrenia na ochranu organizácií na celom svete. Práve vďaka nim má FortiGuard na svojom konte vyše 560 zistení zero-day útokov, čo je rekord, ktorý nedosiahol žiadny iný dodávateľ bezpečnostných riešení.

Každý deň z globálnych produktov a senzorov prijímame vyše 50 miliárd bezpečnostných udalostí, čo je nebývalý objem dát, ktoré poskytujú jasný obraz celosvetového prostredia hrozieb. Jedinečnou kombináciou interného výskumu v 10 rôznych bezpečnostných disciplínach, výmeny informácií s poprednými zdrojmi v odvetví a strojového učenia dosahujeme, že bezpečnostné riešenia Fortinet rutinne získavajú také vysoké hodnotenie v testoch bezpečnostnej účinnosti v reálnom svete vykonávaných inštitúciami ako napríklad NSS Labs, Virus Bulletin, ICSA Labs a AV-Comparatives.

FortiCare

Bezpečnosť môže byť komplexná – vytvorenie prostredia s najlepšou bezpečnosťou vyžaduje skúsenosti. Spoločnosť Fortinet sa venuje bezpečnosti každý jeden deň, pričom naši profesionáli poznajú naše produkty do podrobností. Dokážeme zvýšiť obranné schopnosti ktorejkoľvek IT organizácie prostredníctvom množstva ponúk a prispôsobiť naše služby veľkosti organizácie a želanej úrovni asistencie a monitoringu. Môžeme vám pomôcť zaistiť primeranosť bezpečnostnej pozície vášho zákazníka voči dnešnému vyvíjajúcemu sa prostrediu hrozieb.

Služby FortiCare sú dostupné pre všetky produkty značky Fortinet a obsahujú štyri druhy ponúk:

- **Služby produktovej podpory** zahŕňajú pomoc pri technických problémoch so zariadením, aktualizáciu mikroprogramového vybavenia a v prípade potreby výmenu produktu. K dispozícii je aj monitorovanie zariadení a zasielanie správ o zariadeniach. Pomoc možno poskytovať telefonicky, e-mailom a cez chat.
- **Pokročilé služby podpory** poskytujú podporu individuálne pre konkrétneho klienta, pričom zahŕňajú poradenstvo pri konfigurácii a hodnotenie výkonnosti, ako aj školiace a certifikačné programy. Služba má varianty „Enterprise“ a „Service Provider“.
- **Profesionálne služby** ponúkajú certifikovaných odborníkov na realizáciu školení, návrhov, konfigurácie, implementácie a validácie bezpečnostných produktov a produktov infraštruktúry na mieste. Tieto činnosti sú vytvárané individuálne a vyžadujú súpis prác, aby sa dali správne dimenzovať.
- **Prémiové služby vrátenia a výmeny tovaru** zahŕňajú rozšírenú možnosť vrátenia tovaru na základe záruky s cieľom zrýchlenia celého procesu výmeny, ale aj možnosti bezpečnej likvidácie pre zákazníkov s vysokým štandardom bezpečnosti.

NÁSTROJE PREDAJA

Ako pomôcku pre vašich potenciálnych zákazníkov pri hodnotení ich aktuálnej bezpečnostnej pozície ponúkame niekoľko testov a iných nástrojov, ako aj demonštračné verzie súboru produktov značky Fortinet.

Program hodnotenia kybernetických hrozieb

Náš program hodnotenia kybernetických hrozieb Cyber Threat Assessment Program (CTAP) je predpredajný nástroj, ktorý vašim perspektívnym zákazníkom ponúka rýchly, jednoduchý a cenný pohľad na ich vlastnú bezpečnostnú pozíciu. Pomáha vám získať dôveru, etablovať sa do pozície dôveryhodného poradcu a vypracovať silný obchodný prípad na výber produktov značky Fortinet s cieľom zmierňovania vplyvov hrozieb.

CTAP vďaka miere získavania zákazníkov 85 % predstavuje osvedčenú metódu, ako zmeniť potenciálneho záujemcu bez predchádzajúceho vzťahu na dlhodobého zákazníka a zároveň umožňuje demonštrovať prínosy bezpečnostnej architektúry Fortinet Security Fabric v sieťovom prostredí vášho perspektívneho zákazníka.

Internet: <https://ctap.fortinet.com>

Test Your Metal

Útočníci obchádzajú bezpečnostné opatrenia tak, že malvér skrývajú hlboko v komprimovaných súboroch. Nanešťastie, väčšina sieťových bezpečnostných riešení sa pravidelne necháva oklamať touto technikou, lebo nedokáže analyzovať súbory komprimované v inom formáte ako ZIP. Existuje niekoľko legitímnych, bežne používaných formátov kompresie mimo formátu ZIP, ktoré bežní koncoví používatelia vedia vo väčšine operačných systémov jednoducho otvoriť (napr. TAR, GZ, 7Z, CAB).

Program otestovania vášho systému **Test Your Metal** ponúka jednoduchý test, či vaša sieťová bezpečnosť dokáže zachytiť malvér skrývajúci sa v komprimovaných súboroch.

Internet: <http://metal.fortiguard.com>

Sieťové testovanie

Pomôžte svojim zákazníkom dostať z ich sieťových zariadení maximum a diagnostikovať potenciálne problémy s komplexným testovaním výkonnosti.

FortiTester ponúka súbor silných, ale ľahko obsluhovateľných testov, ktoré simulujú široké spektrum typických podmienok prevádzky. Umožňuje nastavovať výkonnostné štandardy a spúšťať audity na účel kontroly, či ich vaša sieť aj naďalej spĺňa. Taktiež kvôli lepšiemu porovnaniu ukladá testy vykonané v minulosti.

Internet: <http://docs.fortinet.com/fortitester/>

Product Demo Center

Nech sa vaši perspektívni zákazníci sami presvedčia, ako im naše riešenia môžu pomôcť pri riešení ich bezpečnostných problémov. Naše Product Demo Center ponúka širokú škálu produktov Fortinet, aby zákazníkom pomohlo preskúmať ich kľúčové vlastnosti a funkcionality a tiež získať vlastnú skúsenosť z používania našich intuitívnych používateľských rozhraní.

Internet: <http://www.fortidemo.com>

ŠKOLENIE

Školenie Network Security Expert (NSE) je osemstupňový certifikačný program určený pre odborníkov – technikov, ktorí majú záujem o nezávislé zhodnotenie svojich schopností a skúseností v oblasti sieťovej bezpečnosti. Zahŕňavateľné množstvo kurzov a cvičení na budovanie skúseností, ktoré možno absolvovať vlastným tempom alebo pod vedením inštruktora, určených na osvojenie komplexných koncepcií sieťovej bezpečnosti. Školenie NSE tvorí dôležitú súčasť programu FortiPartner, lebo umožňuje partnerom overiť si svoje schopnosti a skúsenosti v oblasti sieťovej bezpečnosti, využiť kompletnú škálu bezpečnostných produktov Fortinet a pomôcť pri rozvoji predaja a ponuke nových služieb. Časť programu sa partnerom ponúka zdarma na internete a sú k dispozícii na partnerskom portáli Fortinet Partner Portal.

Internet: <https://www.fortinet.com/support-and-training.html>

Rýchly školiaci program Fortinet Fast Track Program bol navrhnutý pre partnerov na všetkých skúsenostných úrovniach. Pozostáva z krátkych, ale vyčerpávajúcich kurzov, ktoré pokrývajú najnovšie dôležité témy a výzvy v oblasti kybernetickej bezpečnosti. Účastníci programu si rozvíjajú svoje zručnosti a vedomosti, ktoré im pomôžu odborne reagovať na bezpečnostné problémy zákazníkov.

Ak máte o tento program záujem, obráťte sa, prosím, na vášho miestneho zástupcu spoločnosti Fortinet.



PARTNERSKÁ PODPORA

Spoločnosť Fortinet ponúka svojim partnerom nepreberné množstvo prostriedkov vrátane služieb ako napríklad predajné a produktové školenia, identifikácia príležitostí a pokročilá technická podpora v rámci predpredajného procesu.

Podnikoví zákazníci zvyknú mať špecializované potreby s mnohými komplexnými črtami. Naše globálne tímy manažérov pre vzťahy a predajných technikov sú pripravené, aby vám pomohli s ktorýmkoľvek riešením uvedeným v tejto príručke.

Firemná stránka

<http://www.fortinet.com>

Partnerský portál Fortinet

<https://partnerportal.fortinet.com>

Informácie o školeniach

<http://www.fortinet.com/training/index.html>

Informácie o produktoch

<http://www.fortinet.com/products/index.html>

Knižnica ikon Fortinet-u

Dostupná v časti *Resources* (Materiály) na adrese

<https://www.fortinet.com/resources>

Spojená komunita

<https://fusecommunity.fortinet.com>



Táto príručka predaja je určená pre partnerov spoločnosti Fortinet na účely vzdelávania a získavania kompetencií v oblasti našich špičkových riešení sieťovej bezpečnosti. Dokument nie je vhodný pre zákazníkov.



Copyright © 2018 Fortinet, Inc. Všetky práva vyhradené. Fortinet®, FortiGate®, FortiCare® a FortiGuard®, ako aj niektoré ďalšie značky sú registrovanými ochrannými známkami spoločnosti Fortinet, Inc., pričom iné názvy Fortinet uvádzané v tomto dokumente môžu tiež byť registrovanými, resp. neregistrovanými ochrannými známkami spoločnosti Fortinet. Všetky ostatné názvy produktov a spoločností môžu byť ochrannými známkami svojich príslušných vlastníkov.