FORTINET

Q4 / 2022

Konvergencia sietí a bezpečnosti

FORTINET

Výsledky za fiškálny rok 2021

Tržby
$3,34 mld.

Fakturácia
$4,18 mld.

Q3 2022 Výsledky

Tržby
$1,15 mld.

Fakturácia
$1,411 mld.

Prev. marža (GAAP)
23,1%

EPS (GAAP)
$0,29/akcia

Hotovosť + investície
$1,814 mld.

Kapitalizácia
$38,3 mld.
(k 30. septembru 2022)

Zákazníci

viac ako 615 tis.

Celkovo dodaných jednotiek

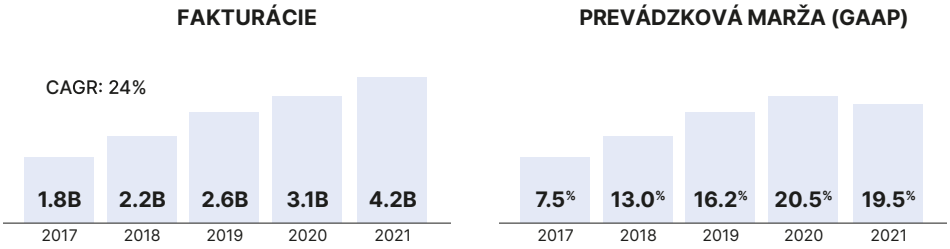
viac ako 9,4 mil.

Počet zamestnancov podľa regiónu

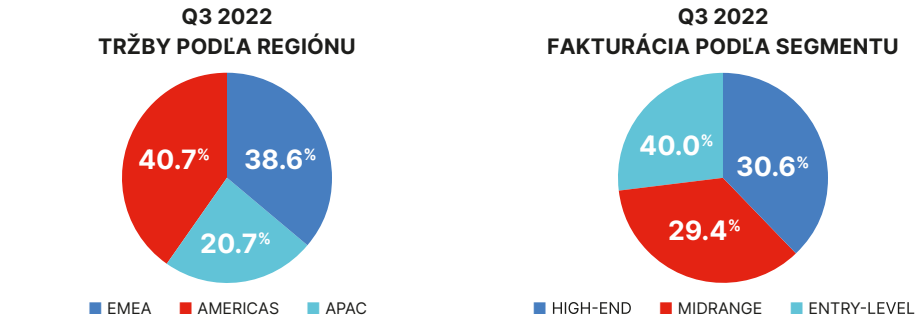
AMERICAS	USA	3 603
	Kanada	2 257
	Zvyšok regiónu	867
EMEA	Francúzsko	484
	Veľká Británia	400
	Zvyšok regiónu	2 049
APAC	India	616
	Japonsko	526
	Zvyšok regiónu	1 289
Spolu		12 091

Všetky údaje sú platné k 30. 8. 2022

Silný medziročný nárast fakturácií a výnosnosti

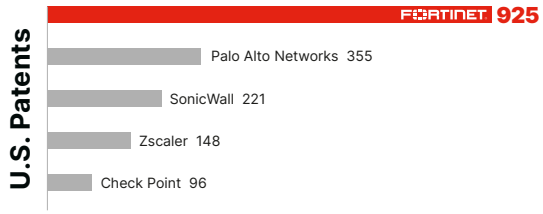


Vysoká diverzifikácia naprieč regiónmi a segmentmi



Technologické líderstvo

Takmer 3-krát viac patentov ako porovnateľné spoločnosti ponúkajúce riešenia v oblasti zabezpečenia sietí



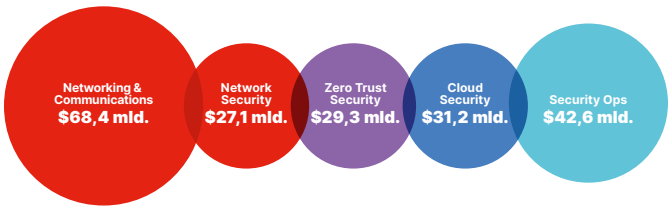
Zdroj: patentový úrad v USA, k 30. septembru 2022

1285
globálnych patentov

925 patentov v USA
360 patentov medzinárodne
(250 patentov čakajúcich na schválenie)

Veľký a rastúci celkový dostupný trh

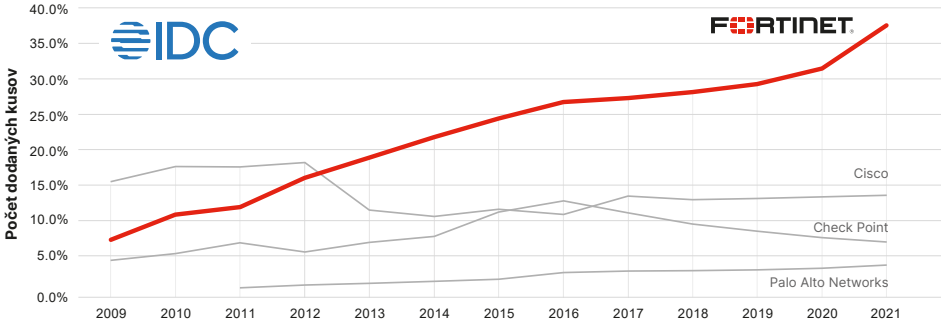
Celkový adresovateľný trh s hodnotou 138 mld. dolárov z roku 2022 stúpne na 199 mld. dolárov do roku 2026



Zdroj: Odhady Fortinetu založené na nedávnom analytickom výskume. Zobrazená príležitosť pre 2026.

Najčastejšie nasadzované riešenie zabezpečenia siete

Viac ako tretina z celkového počtu dodaných firewallov



Zdroj: IDC Worldwide Security Appliance Tracker, marec 2022 (na základe počtu ročne dodaných kusov zariadení Firewall, UTM a VPN)

Fortinet - umožňujeme chod digitálneho sveta, ktorému môžete dôverovať

Fortinet je už viac ako 20 rokov hybnou silou vo vývoji kybernetickej bezpečnosti a konvergencie sietí a zabezpečenia. Naše riešenia zabezpečenia siete sú najrozšírenejšie, najpatentovanejšie a patria k najoverenejším v odvetví. Naše široké, doplnkové portfólio riešení pre kybernetickú bezpečnosť je postavené od základov tak, aby kládlo dôraz na integráciu automatizáciu, čo umožňuje efektívnejšie samo-ošetrujúce operácie a rýchlu reakciu na známe aj neznáme hrozby.

Investing in Global Scale

- Vlastníctvo nehnuteľností s rozlohou viac ako 185 tis. m^2 znamená, že investujeme so zreteľom na dlhodobý ekonomický rast
- Zaviazali sme sa, že do roku 2030 dosiahneme uhlíkovú neutralitu
- Máme novú a modernú centrálu s rozlohou 16 000 m^2 a s LEED-Gold certifikáciou.

Misia: zabezpečiť ľudí, zariadenia a dáta nech sú kdekoľvek

Založený: Október 2000

Centrála: Sunnyvale, Kalifornia

Fortinet IPO (FTNT): November 2009

NASDAQ 100 and S&P 500:
Jediná spoločnosť zameraná na kyberbezpečnosť zaradená v oboch indexoch

Investícia do budúcnosti **$10 mld.** fakturácia **do roka 2025**

Korporátna spoločenská zodpovednosť

Viac informácií na **fortinet.com/CSR**

Digitálny svet, ktorému môžete vždy dôverovať, je nevyhnutný na dosiahnutie spravodlivých a udržateľných spoločností. Vo Fortinete veríme, že je našou korporátnou spoločenskou zodpovednosťou (CSR) pričiniť sa o dosiahnutie tejto vízie inováciou udržateľných bezpečnostných technológií a diverzifikáciou kybernetickej bezpečnosti. Zároveň podporujeme zodpovedné podnikanie v celom našom hodnotovom reťazci.

Inováciou k bezpečnému Internetu

Rozširovanie inkluzívnej pracovnej sily dbajúcej na kybernetickú bezpečnosť

Rešpekt k životnému prostrediu

Podpora zodpovedného podnikania

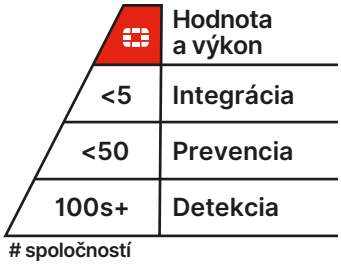
Hlavné výhody Fortinetu

Security Fabric

Organicky vyvinutá, vysoko integrovaná a automatizovaná platforma kybernetickej bezpečnsti

Procesory zabezpečenia

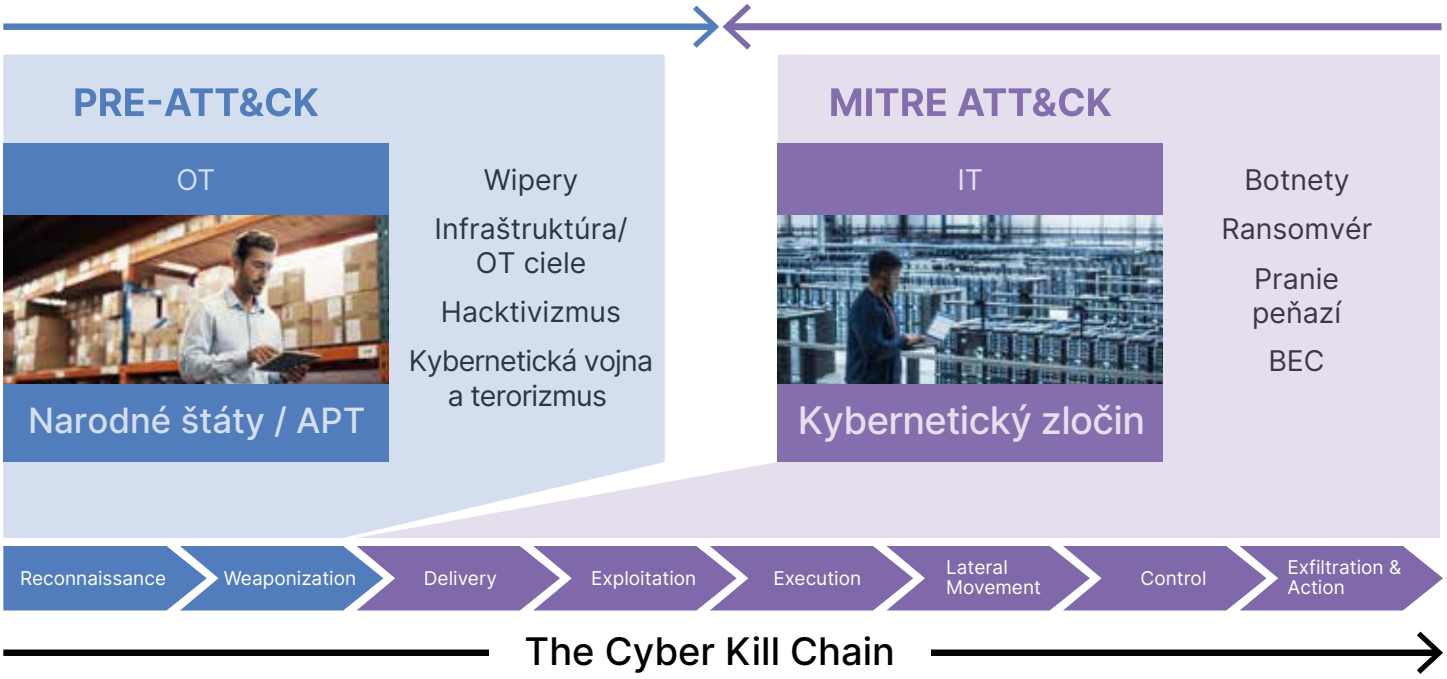
Prvotriedny NGFW a výkon a efektívnosť SD-WAN-u



Jediná spoločnosť, ktorá exceluje vo všetkých kľúčových fázach bezpečnosti siete

Rozširujúci sa útočný povrch zvyšuje kybernetické riziko

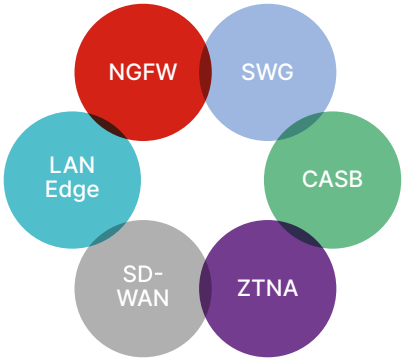
Kyberzločinci sa tradične zameriavajú na využívanie útočných metód podrobne opísaných v rámci frameworku MITRE ATT&CK, ku ktorým patria napr. získanie prístupu, eskalácia privilégií či nastolenie hrozby. Avšak pri pokročilých perzistentných hrozbách (APT) útočníci zvyčajne využívajú metódy spred samotného útoku, teda sa zameriavajú na prípravné fázy, ktoré im umožnia zotrvať v zacielenom zariadení alebo sieti (ako je uvedené vo frameworku MITRE PRE-ATT&CK). Kyberzločinci si však začali osvojovať taktiku a technológie podobné APT s cieľom vyvíjať a rozširovať útoky rýchlejšie, ako doposiaľ. A využívajú pritom model Cybercrime-as-a-Service na zrýchlenie miery exploitov zameraných na dnešný rozširujúci sa povrch digitálnych útokov.



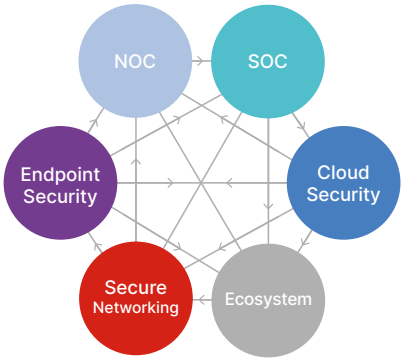
Konsolidujte bodové produkty kybernetickej bezpečnosti a tvorby siete

Tradičný prístup pokiaľ ide o riešenie sieťových alebo bezpečnostných problémov spočíva v nájdení riešenia pre konkrétnu výzvu a následne v nasadení daného riešenia. Výsledkom je čoraz zložitejšie prostredie, v ktorom je ťažké sa orientovať, spravovať ho a zabezpečiť ho. A tento problém sa pri rozšírení siete ešte znásobuje, čo jednoducho znamená, že udržiavanie konzistentného bezpečnostného profilu sa stáva čoraz ťažším, a to najmä vtedy, ak nástroje nie sú navrhnuté tak, aby spolupracovali. Spoločnosť Fortinet rieši túto výzvu konvergenciou sieťových a bezpečnostných funkcií v jedinom operačnom systéme FortiOS, ktorý je najrozšírenejším a najvyspelejším operačným systémom v odvetví. Tento prístup umožňuje IT tímom spravovať sieťové a bezpečnostné politiky prostredníctvom jediného riešenia, čím sa používateľský komfort a bezpečnosť stávajú konzistentnými bez ohľadu na to, kde sa nachádzajú pracovníci alebo kde sa nasadzujú aplikácie. Znížením zložitosti sa zároveň odstránia medzery v zabezpečení, zvýši sa prevádzková efektívnosť a znížia sa celkové náklady na vlastníctvo.

Konvergencia sietí a bezpečnosti



Integrovaná platforma kybernetickej bezpečnosti



The Fortinet Security Fabric

Fortinet Security Fabric je jadrom bezpečnostnej stratégie Fortinetu. Je to platforma organicky postavená na spoločnom operačnom systéme a riadiacom rámci. Umožňuje širokú viditeľnosť, bezproblémovú integráciu a interoperatívnosť medzi kritickými bezpečnostnými prvkami a tiež granulárne riadenie a automatizáciu.

Široká

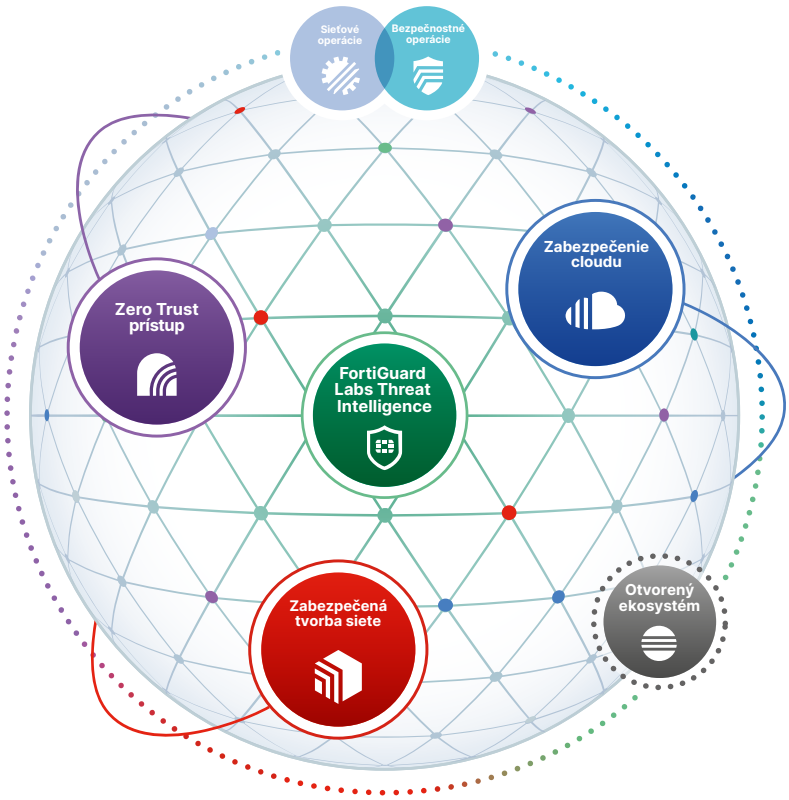
viditeľnosť a ochrana naprieč celým povrchom digitálneho útoku s cieľom lepšie riadiť riziko.

Integrované

riešenie minimalizujúce komplexnosť riadenia, ktoré zdieľa informácie o hrozbách.

Automatizované

samo-ošetrujúce sa siete využívajúce zabezpečenie na princípe AI s cieľom zaistiť rýchle a efektívne operácie.



Viac informácií na **fortinet.com/securityfabric**

Široké portfólio riešení na ochranu povrchu digitálnych útokov

Zero-trust prístup

- Univerzálny ZTNA
- SASE
- CASB
- Identity
- Autentifikácia

Zabezpečená tvorba siete

- Next-Generation Firewall
- Secure SD-WAN
- Ethernet
- Wireless
- 5G/LTE WAN Gateway
- Kontrola prístupu do siete
- a viac

Zabezpečenie cloudu

- Cloudová natívna ochrana
- DevSecOps
- Cloudový Firewall
- SD-WAN pre multi-cloud
- WAF
- Zabezpečenie e-mailov
- ADC/GSLB
- Anti-DDOS

Sieťové operácie

- Centralizovaná správa
- Správa v cloude
- AIOps pre Networking
- Monitorovanie digitálneho zážitku

Bezpečnostné operácie

- Koncové body (EDR/XDR)
- Automatizácia: SIEM/SOAR
- Správa SOC a MDR
- DRPS, EASM
- Podvody

Otvorený ekosystém

- Fabric konektory
- Fabric API
- Fabric DevOps
- Rozšírený ekosystém
- Viac ako 500 otvorených ekosystémov
- Integrácie

LABS

FortiGuard Labs - Popredné Threat Intelligence riešenie v rámci odvetvia

FortiGuard Labs (založená v roku 2002) je elitnou organizáciou Fortinetu zameranou na výskum a spravodajstvo o kybernetických hrozbách. Organizácia spolupracuje s orgánmi činnými v trestnom konaní, vládnymi organizáciami a alianciami dodávateľov bezpečnostných riešení na celom svete, aby bojovala proti novovznikajúcim globálnym bezpečnostným rizikám. FortiGuard Labs poskytuje informácie o hrozbách ako aj inovatívne praktiky a nástroje prevencie v reálnom čase naprieč Fortinet Security Fabric v troch kľúčových kategóriách:

Dôveryhodné ML a AI

Zastavte cudzie prvky promptnejšie vďaka výkonnej kombinácii vykonateľného učenia v danej lokalite a AI a ML modelom vo veľko-škálových cloudových dátových jazerách

Threat management v reálnom čase

Proaktívny bezpečnostný postoj prostredníctvom nepretržitých bezpečnostných aktualizácií založených na internom prehľadávaní a spolupráci

Vyhľadávanie hrozieb a upozornenia o napadnutí

Rýchlejšia náprava vďaka výstrahám, analýze a detekcii, prevencii a nástrojoch nápravy (vrátane ohnísk)

Globálne líderstvo a spolupráca: CYBER THREAT ALLIANCE, WORLD ECONOMIC FORUM, INTERPOL, NCI AGENCY

FortiGuard: zabezpečenie poháňané AI

Táto bohatá paleta špičkových bezpečnostných schopností bola zjednotená do jedného bezpečnostného rámca s cieľom poskytnúť koordinované a kontextu znalé zásady pre hybridné nasadenia v sieťach, koncových bodoch a cloudoch. Tieto služby neustále vyhodnocujú riziko a automaticky prispôsobujú prevenciu, aby čelili známym a neznámym hrozbám v reálnom čase.

Popredné Security-as-a-Service riešenie na trhu

Zabezpečenie s podporou ML, nasadené v blízkosti chránených aktív poháňané FortiGuard Labs

Konzistentné zásady znalé kontextu

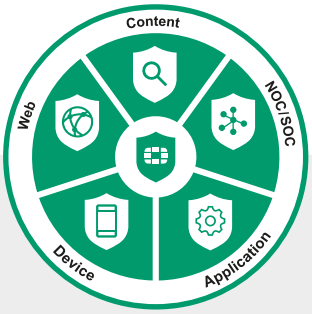
Centralizovaná detekcia a prevencia poskytovaná z cloudu a vytvorená pre hybridné prostredia

Koordinovaná prevencia v reálnom čase

Neustále vyhodnocovanie rizík a automatická reakcia a kontrovanie známym a neznámym hrozbám

Integrácia FortiGuard Security naprieč Security Fabric

		FortiGate (HW/VM/SASE)	Proxy	FortiTrust	XDR	FortiWeb	FortiMail	FortiADC	SOC Platforms	FortiNDR
Zabezpečenie obsahu	Antivirus	✓	✓	✓	✓	✓	✓	✓		✓
	IL SBX	✓			✓	✓	✓	✓		
	Credential Stuffing	✓	✓			✓		✓		
Zabezpečenie webu	URL	✓	✓	✓	✓	✓	✓			✓
	DNS	✓	✓	✓	✓					
	IP-REP	✓				✓	✓			
Zabezpečenie zariadení	DVC PROT	✓								
	IPS	✓	✓	✓						✓
	BOT/C2	✓	✓	✓	✓		✓			
Zabezpečenie aplikácií	WAF SIG					✓				
	ANN							✓		
	AntiSpam						✓			
Zabezpečenie SOC	MITRE ATT&CK				✓				✓	
	Threat Hunting				✓				✓	
	Auto IR				✓				✓	
	Outbreak							✓	✓	✓
	IoC				✓				✓	✓



Nové prvky FortiOS 7.2

NOVÝ FortiSandbox Inline Blocking

NOVÁ IoT/ IT ochrana zariadenia

NOVÝ dedikovaný IPS systém

NOVÝ SOC as a Service

NOVÁ detekcia ohnísk napadnutí

Vylepšené zabezpečenie webu

V našom obsiahlom portfóliu s riešeniami Security Fabric je k dispozícii viacero predplatených služieb FortiGuard

Viac informácií nájdete na **fortinet.com/fortiguard**

FortiOS – Základ Security Fabric

Viac informácií nájdete na **Fortinet.com/fortiOS**

FortiOS je základom Fortinet Security Fabric, ktorý konverguje a konsoliduje mnoho bezpečnostných a sieťových technológií a prípadov použitia do zjednodušeného a jednotného rámca opatrení a riadenia.

Aké nové prvky ponúka FortiOS 7.2

FortiGate SD-WAN
Automatizovaná orchestrácia prekrytia a široko-škálový Zero-Touch provisioning

FortiGate Firewall
FortiGate je firewall ďalšej generácie na podporu HTTP/3.0

SD-Branch
Automatizácia, zjednodušené nasadenie a orchestrácia umožňujúce globálne škálovanie

LAN Edge
Zero-Touch provisioning Campus a veľko-škálová SD-Branch

ZTNA
Konfigurácia jednotnej politiky v jedinom GUI

FortiToken / FortiToken Cloud
Autentifikácia bez hesla cez Fido

SASE
Automatizované poskytovanie (provisioning) agentov a aplikácií ZTNA prostredníctvom FortiSASE

Identita
Zero Touch Provisioning Campus a rozsiahly SD-Branch

FortiTrust – nový pohľad na budúcnosť služieb zabezpečenia

FortiTrust poskytuje užívateľské licencovanie vo všetkých sieťach, koncových bodoch a cloudoch

- **Prístup:** Pridajte ZTNA do svojej siete s FortiGate-om
- **Identita:** Predplatné cloudových riešení v hybridnom podnikovom prostredí

FortiCare – Expertíza k vašim službám

Viac informácií na **Fortinet.com/support**

Služby FortiCare pomáhajú tisícom organizácií každý rok naplno využiť riešenia Fortinet Security Fabric. Máme viac ako 1 400 expertov poskytujúcich zrýchlenú implementáciu, spoľahlivú pomoc, a proaktívnu starostlivosť prostredníctvom pokročilej podpory a profesionálnych služieb s cieľom maximalizovať vaše zabezpečenie a výkon.

1400+ EXPERTOV

24×7 TECHNICKÁ PODPORA

23 CENTIER PODPORY CELOSVETOVO

Prijatie nových technológií nie je projekt so začiatkom a koncom. Je to predovšetkým cesta od dizajnu a implementácie po optimalizáciu, prevádzku a neustálu správu riešenia. Fortinet zastrešuje každý krok na tejto ceste a odľahčuje vaše zdroje, aby ste sa mohli plne zamerať na potreby svojho podnikania.

Dizajn

Zadefinovanie obchodných potrieb
- Dizajn vysokej úrovne
- Dizajn nízkej úrovne
- Workshopy zamerané na kompatibilitu systémov

Nasadenie

Urýchlená implementácia
- Migrácia
- Konfigurácia
- Implementácia
- Validácia
- Transfer poznatkov

Prevádzka

Spoľahlivá asistencia
- Podpora 24/7
- Výmena za prémiový hardvér
- Správa technického účtu
- Proaktívne vyhnutie sa incidentom
- Dedikované zdroje

Optimalizácia

Výkonnostná excelentnosť
- Kontroly zdravia (stavu)
- Odporúčania aktualizácie softvéru
- Pripravenosť na incident
- Testovanie penetrácie

Evolúcia

Personalizovaná starostlivosť
- Asistencia pri aktualizovaní produktov
- Príprava na transformáciu
- Migrácia a náhrada
- Upgrade softvéru

Výhody SPU

Bezpečnostné procesory (SPU) od Fortinetu radikálne navyšujú rýchlosť, rozsah, efektívnosť a hodnotu riešení od Fortinetu pričom výrazne zlepšujú používateľskú skúsenosť a znižujú stopu a požiadavky na výkon. Od entry-level úrovne po pokročilé riešenia: zariadenia poháňané SPU procesormi od Fortinetu zaisťujú vynikajúci rating čo sa zabezpečenia týka v porovnaní s inými alternatívami v rámci odvetvia.

Network Processor 7
NP7

Network Processors operate in-line to deliver unmatched performance for network functions and hyperscale for stateful firewall functions.

Content Processor 9
CP9

As a co-processor to the main CPU, Content Processors offload resource-intensive processing and drive content inspection to accelerate security functions.

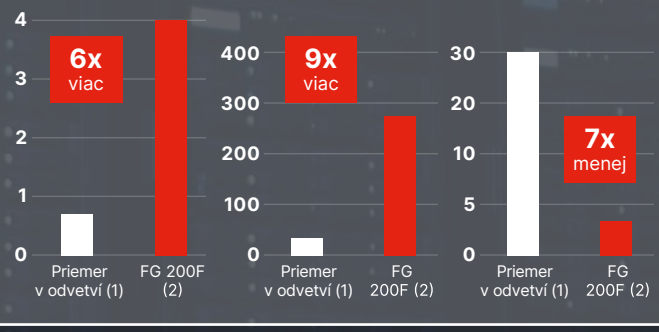
System-on-a-Chip 4
SoC4

The System-on-a-Chip consolidates network and content processing, delivering fast application identification, steering, and overlay performance.

Bezpečnostné výpočtové hodnotenia (security compute rating) sú benchmarky, ktoré porovnávajú výkonové metriky firewallov novej generácie poháňaných Fortinet SPU procesormi s riešeniami s podobnými cenami od dodávateľov, ktorí na networking a zabezpečenie používajú generické procesory.

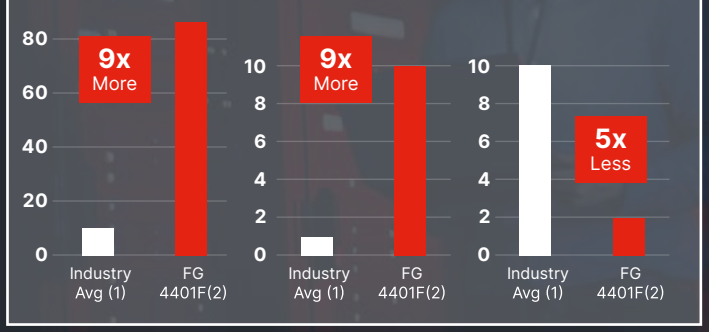
Entry-level zariadenia

SoC4



Pokročilé zariadenia

NP7 CP9



[1] Priemer v odvetví (entry level) sa vypočíta ako priemer podobne nacenených modelov PAN-820, Cisco FPR-1120, Juniper SRX-345 a Check Point SG-3600. Priemer v odvetví (high-end/pokročilý) sa vypočíta ako priemer podobne nacenených modelov PAN-7050, Cisco FPR-9300, Juniper SRX-5400 a Check Point SG-28000. Všetky údaje z verejných technických listov.
[2] Metriky Fortinetu z verejných technických listov.

Nový produkt na scéne: FortiGate 1000F/1001F

Vyšší výkon, nižšia spotreba energie

O 80 % nižšia spotreba energie v porovnaní s konkurenciou

Ultraškálovateľné a vysoko výkonné zabezpečenie

Ochrana kritických údajov pomocou riešenia FortiGuard poháňaného AI

Špecifikácia	FortiGate 1000F[1]	Security Compute Rating	Priemer v odvetví	Palo Alto Networks PA-3420	Check Point Quantum 6700	CISCO FIREPOWER 2140	JUNIPER SRX 4100
Priepustnosť firewallu	198 Gbps	**7.4 X**	26.7 Gbps	20.8 Gbps	26 Gbps	20 Gbps	40 Gbps
Priepustnosť IPsec VPN	55 Gbps	**6.7 X**	8.1 Gbps	9.9 Gbps	4.6 Gbps	3.6 Gbps	14.8 Gbps
Ochrana pred hrozbami[2]	13 Gbps	**2 X**	6.7 Gbps	7.6 Gbps	5.8 Gbps	N/A	N/A
Konkurentné relácie	7.5 M	**2.5 X**	3 M	2 M	2 M	3 M	5 M
Pripojenia za sekundu	650 K	**3.7 X**	173.5 K	205 K	164 K	75 K	250 K
Priepustnosť firewallu watty/Gbps	2.06 W	**6.0 X**	12.46 K	11.5 W	7.3 K	20 W	11.0 W
Priepustnosť IPsecVPN watty/Gbps	7.42 W	**7 X**	51.5 K	24.2 W	41.0 W	111.1 W	29.7 W
BTU/h na Gbps priepustnosti firewallu	6.2 BTU	**6.5 X**	40.45 BTU	31.3 BTU	24.8 BTU	68.2 BTU	17.2 BTU

Poznámky:
1. K dispozícii je aj variant bez SSD
2. Ochrana pred hrozbami zahŕňa kontrolu aplikácií FortiGuard, AI-poháňané FortiGuard IPS, antivírus, logovacie a sandboxové bezpečnostné služby.
3. Všetky hodnoty spotreby energie sú prevzaté z externých dátových listov a hardvérových systémových príručiek s použitím maximálnej spotreby energie

Školenie a certifikácia

Fortinet NSE Certification Program

Program Fortinet Network Security Expert (NSE) je 8-úrovňový školiaci a hodnotiaci program určený pre zákazníkov, partnerov, zamestnancov a profesionálov z oblasti IT. Stanovuje si cieľ podporiť zručnosti v oblasti kybernetickej bezpečnosti. Doposiaľ bolo udelených viac ako 1 milión bezpečnostných certifikátov. Fortinet týmto spôsobom poskytuje expertné školenie v miestnych jazykoch online vo viac ako 136 krajinách a územiach celosvetovo za pomoci autorizovaných školiacich centier.

Fortinet Training & Education Partner Programs

Ekosystém verejných a súkromných partnerstiev Fortinet Training Institute pomáha spoločnosti Fortinet pri zameraní sa na medzeru v zručnostiach, a to zvýšením prístupu a dosahu našich certifikácií a školení v oblasti kybernetickej bezpečnosti. Akademický partnerský program spolupracuje s akademickými inštitúciami vrátane K-12 a vyššieho vzdelávania. Program Education Outreach Program spolupracuje s odvetvím, akademickou obcou, vládami a neziskovými organizáciami, aby oslovil širokú populáciu, pričom sa zameriava aj na nábor žien, menšín a veteránov.

1,000,000+
CERTIFIKÁCIÍ

498
AKADÉMIÍ

31
PARTNEROV V OBLASTI VZDELÁVANIA

Povedomie o informačnej bezpečnosti

Oboznámte sa so súčasnými kybernetickými hrozbami a o tom, ako môžete zabezpečiť svoje informácie.

Spolupracovník

Oboznámte sa s jednotlivými riešeniami zabezpečenia, ktoré boli vytvorené s cieľom predchádzať bezpečnostným ťažkostiam v organizáciách.

Spolupracovník

Oboznámte sa s kľúčovými produktmi spoločnosti Fortinet a problémami kybernetickej bezpečnosti, na ktoré sa zameriavajú.

Profesionál

Rozšírte si znalosti potrebné pri správe každodennej konfigurácie, monitorovania a prevádzky zariadení FortiGate a podporte tak bezpečnostné politiky podnikovej siete.

Analytik

Detailne pochopiť, ako implementovať riadenie bezpečnosti siete a analýzy.

Špecialista

Porozumieť technickej stránke zavádzania systémov pre riadenie a analýzu sieťovej bezpečnosti do hĺbky.

Architekt

Rozvíjať vedomosti o integrácii produktov Fortinet na nasadenie a správu bezpečnostných riešení siete.

Expert

Preukázať schopnosť navrhovať, konfigurovať, inštalovať a riešiť problémy komplexných sieťových bezpečnostných riešení v prostredí prevádzky.

Viac informácií na **fortinet.com/nse-training**

Údaje sú z 30. septembra 2022

Nová služba spoločnosti Fortinet zameraná na zvyšovanie povedomia o bezpečnosti a školenia

Služba zameraná na povedomie o bezpečnosti a školenia ponúka každej organizácii možnosť ďalej chrániť svoje kritické digitálne aktíva pred kybernetickými hrozbami prostredníctvom budovania povedomia zamestnancov o kybernetickej bezpečnosti a vytvárania kultúry kybernetického povedomia.

Bezplatné školenia a zvyšovanie povedomia o kybernetickej bezpečnosti vo všetkých školských obvodoch v USA

Od konania Národného summitu o pracovnej sile a vzdelávaní (júl 2022) Fortinet ponúka prispôsobenú verziu svojej služby zameranej na zvyšovanie bezpečnostného povedomia a školení všetkým z ôsmich miliónov zamestnancov a pedagógov v školských obvodoch a systémoch v USA. Tento príspevok je súčasťou poslania spoločnosti Fortinet, ktorá chce týmto spôsobom prispieť k odstráneniu medzier v zručnostiach v oblasti kybernetickej bezpečnosti.

Náš záväzok vyškoliť 1 milión ľudí do roku 2026

Fortinet sa zaviazal vyškoliť 1 milión ľudí na celom svete počas nadchádzajúcich 5 rokov prostredníctvom svojich programov Training Advancement Agenda a NSE Training Institute, aby prispel k zvládnutiu medzery v zručnostiach v oblasti kybernetickej bezpečnosti. Tento päťročný záväzok platí od januára 2022. Počas tohto obdobia sa bude ako základ pre naplnenie tohto cieľa využívať ocenený obsah certifikačného programu Fortinet. Fortinet Training Institute bol ocenený rôznymi organizáciami za náš príspevok k excelentnosti, čo sa týka školení a certifikácie v oblasti kybernetickej bezpečnosti, ako aj za naše početné programy, ktoré pomáhajú pri zmenšovaní medzery v zručnostiach v oblasti kybernetickej bezpečnosti.

Náš globálny partnerský záväzok

Fortinet je spoločnosť zameraná na kanály. Vytvorili sme veľkú globálnu sieť dôvery-hodných poradcov, na ktorých sa zákazníci môžu spoľahnúť čo sa týka zabezpečenia svojej digitálnej transformácie a strategického riadenia obchodného rastu.

ENGAGE FORTINET PARTNER PROGRAM

VIAC AKO **60 000** AKTIVNÝCH PARTNEROV

Program Engage Partner Program je navrhnutý tak, aby partnerom pomohol vybudovať hodnotnú a vysoko diferencovanú a zabezpečenú prevádzku, ktorá využíva najlepšie riešenia v odvetví na podporu úspechu zákazníkov. Globálny partnerský program spoločnosti Fortinet sa riadi tromi základnými konceptmi:

Rast prostredníctvom diferenciácie technológií

Škála produktov spoločnosti Fortinet je úzko integrovaná do jednej vysoko automatizovanej, vysoko výkonnej platformy, ktorá zahŕňa koncový bod, sieť, a cloud, a obsahuje nástroje na jednoduché prepojenie s hraničiacimi technológiami.

Obchodný úspech s osvedčenou dôveryhodnosťou

Špičkové technologické inovácie spoločnosti Fortinet a vedúce postavenie v odvetví čo sa týka spravodajstva o hrozbách, spolu s hodnoteniami od našich zákazníkov a nezávislé správy analytikov potvrdzuje a diferencuje ponuky našich partnerov.

Dlhodobý, udržateľný rast

Program Engage Partner Program ponúka udržateľný predaj, marketing, a exekutívnu podporu, aby ste mohli vytvárať produktívne, predvídateľné, a úspešné vzťahy. Vďaka hnacím silám rastu integrovanými do programu, ako sú naše Špecializácie, poskytujeme prístup k odbornosti pre riešenia, ktoré poháňajú dopyt na trhu, a zaisťujú, že vaše smerovanie povedie k úspechu.

- SPECIALIZATION: SD-WAN
- SPECIALIZATION: Zero Trust Access
- SPECIALIZATION: Security Operations
- SPECIALIZATION: Data Center
- SPECIALIZATION: Operational Technology
- SPECIALIZATION: Cloud Security
- SPECIALIZATION: LAN Edge and SD-Branch

Hodnotenie analytikov

Gartner — Magic Quadrants: 7
- Sieťový firewall
- SD-WAN
- Wired a WLAN
- Koncový bod
- SIEM
- WAAP v cloude
- Vnútorné umiestnenie Služby

Gartner — Market Guides: 9
- SASE od jedného predajcu
- DEM
- IRM
- VPN
- XDR
- NAC
- SOAR
- E-mail
- Aplikácia s vnútorným umiestnením služieb

Gartner — #1 in Critical Capabilities: 5

Sieťový firewall
- Okraj dátového centra
- Distribuovaný okraj

SD-WAN
- Zabezpečený SD-WAN
- WAN pre malú pobočku
- Vzdialená pracovná sila

Gartner — Peer Insights Customers' Choice: 4
- Sieťový firewall
- Wired a WLAN
- Zabezpečený e-mail
- Infraštruktúra WLAN okraja

Forrester — Waves: 4
- Zabezpečenie podnikových e-mailov
- ICS
- Detekcia koncových bodov a odozva
- Podnikové firewally

Forrester — Nowtechs: 5
- WAF
- All-In-One ZeroTrust Edge
- Softvérom definovaná WAN
- Detekcia koncových bodov a odozva
- Zabezpečenie podnikových e-mailov

Frost & Sullivan — Top Vendor & Leadership Awards: 6
- SD-WAN
- Kritická infraštruktúra
- SWG
- NAC
- WAN Edge infraštruktúra
- Severoamerické zdravotníctvo

IDG — Marketscape Leader & Major Player: 2
- Celosvetová SD-WAN infraštruktúra
- Moderný koncový bod

Westlands Advisory — Platform Navigator: 1
- Bezpečnostná IT/OT platforma

Kuppingercole — Leadership Compass: 2
- SIEM
- ICS

GIGAOM — GIGAOM Radar: 2
- Security Service Access (SSA) - označenie „napredujúci"
- Zero-Trust Network Access (ZTNA) - označenie „rýchlo reagujúci"

Gartner

Fortinet získal uznanie ako líder v 2 správach Gartner® 2021 Magic Quadrant™:

Sieťové Firewally

WAN Edge infraštruktúra

Fortinet získal uznanie v 4 ďalších správach Gartner Magic Quadrant 2021 vrátane širokej škály technológií:

Firewall pre webové aplikácie

SIEM

Drôtová a bezdrôtová sieť LAN

Platformy na ochranu koncových bodov

Fortinet sa tiež spomína ako „predajca na zváženie“ v 2 ďalších správach Gartner Magic Quadrant z roku 2020/2022:

Zabezpečená webová brána

Lokalizačné služby vo vnútornom prostredí

Access Management

Viac informácií na **fortinet.com/solutions/gartner-magic-quadrants**

Testovanie a certifikácie tretími stranami

Fortinet predkladá svoje produkty pre nestranné testovanie výkonu a účinnosti tretím stranám s najprominentnejšími organizáciami v odvetví. Výsledky sú konzistentne pozitívne.

- Jediný predajca so všetkým i tromi certifikáciami VB100, VBSpam a VBWeb
- Najvyššie hodnotenie „VBSpam+“

Certifikované v 5 technologických oblastiach:

- Anti-Malvérová sieť
- Sieťový firewall
- IPsec VPN
- Firewall pre webové aplikácie
- Pokročilá obrana pred hrozbami

- Schválené proti phishingu

100 % Ochrana, 2 roky po sebe

- Vo všetkých testovacích prípadoch
- Všetko nezávislé od podpisu
- Všetko po vybalení z krabice

CUSTOMER RECOGNITION

Status „Gartner Peer Insights Customers's Choice“ je založený na ohodnotení dodávateľov riešení profesionálnymi a overenými koncovými používateľmi z rôznych odvetví a rôznych častí sveta. Výsledné hodnotenie zohľadňuje počet jednotlivých hodnotení od koncových používateľov, ktoré sú dodávateľovi udelené a celkovú známku udelenú dodávateľovi od týchto používateľov.

Fortinet je hrdý na to, že získal označenie „Zákaznícka voľba“ na platforme Gartner Peer Insights a to vo viacerých kritických oblastiach:

Sieťové brány Firewall

Drôtová a bezdrôtová LAN Infraštruktúra

Zabezpečenie emailu

WAN Edge Infraštruktúra

Pozrite si naše hodnotenia a ocenenia na stránke platformy Gartner PeerInsight ***www.gartner.com/reviews***

Gartner, Gartner Peer Insights „Hlas zákazníka“: Network Firewalls, Peer Contributors, 9. apríla 2021

Gartner, Gartner Peer Insights „Hlas zákazníka“: Za infraštruktúru prístupu ku káblovej a bezdrôtovej sieti LAN, Peer Contributors, 12. máj 2021

Gartner, Gartner Peer Insights „Hlas zákazníka“: Za zabezpečenie emailu, Peer Contributors, 5. februára 2021

Gartner, Gartner Peer Insights „Hlas zákazníka“: Za WAN Edge infraštruktúru, Peer Contributors, 5. Februára 2021

Označenie Gartner Peer Insights Customers Choice je ochrannou známkou a servisnou značkou spoločnosti Gartner, Inc. a/alebo jej pridružených spoločností a používa sa tu so súhlasom. Všetky práva sú vyhradené. Gartner Peer Insights Customers' Choice obnáša subjektívne názory vyjadrené prostredníctvom jednotlivých recenzií a hodnotení koncových používateľov a údaje použité podľa dokumentovanej metodiky; nereprezentujú názory ani neobnášajú schválenie spoločnosťou Gartner alebo jej pridruženými spoločnosťami.

Fortinet poskytuje zabezpečenie pre viac ako pol milióna podnikov, poskytovateľov služieb a vládnych organizácií po celom svete.

Piata najväčšia letecká spoločnosť v USA.

Centrála: USA

Najväčšia latinskoamerická sieť fitnescentier s viac ako 1 000 pobočkami a viac ako 3 miliónmi zákazníkov v 13 rôznych krajinách.

Centrála: USA

SoftBank je nadnárodný konglomerát, ktorý sa usiluje o digitálnu transformáciu.

Centrála: Japonsko

Jeden z najväčších svetových producentov kvalitného čerstvého ovocia a zeleniny.

Centrála: USA

University of Birmingham, jedna z najväčších univerzít v Spojenom kráľovstve, s vyše storočnou históriou, má viac ako 30 000 študentov po celom svete.

Centrála: Spojené kráľovstvo

Poskytovateľ online finančných služieb s viac ako 42 miliónmi individuálnych používateľov a s viac ako 300 korporátnymi používateľmi v Hong Kongu, pevninovej Číne a Indonézii.

Centrála: Hong Kong

Globálny líder v oblasti riadených služieb, ktorý poskytuje end-to-end a plne riadenú kybernetickú bezpečnosť, tvorbu sietí a riešenia digitálneho značenia prispôsobené jedinečným obchodným požiadavkám dnešných podnikov.

Centrála: USA

Orange je jedným z popredných svetových telekomunikačných operátorov a globálny poskytovateľ IT a telekomunikačných služieb.

Centrála: Francúzsko

Poskytovateľ flexibilných hybridných IT riešení pre obchodnú sféru a vládu.

HQ: Austrália

Navštívte stránku fortinet.com/customers a pozrite si, koľko našich zákazníkov využíva riešenia Fortinet a Fortinet Security Fabric

Revision: Q4 / 2022 v1 11.01.22