SMLOUVA NA DODÁVKU SOFTWARU

1. Smluvní strany

Masarykův onkologický ústav
se sídlem Žlutý kopec 7, 656 53 Brno
zastoupený prof. MUDr. Markem Svobodou, Ph.D., ředitelem
IČO: 00209805, DIČ: CZ00209805
bankovní spojení: Česká národní banka, číslo účtu: 87535621/0710
(dále také „objednatel“)

a

UNIS COMPUTERS, a. s.
se sídlem Jundrovská 618/31, 624 00 Brno
zastoupený Ing. Vítězslavem Machem, členem představenstva
IČO: 63476223, DIČ: CZ63476223
bankovní spojení: UniCredit Bank Czech Republic and Slovakia a.s., č. ú.: 39921026/2700
zapsaný v obchodním rejstříku vedeném Krajským soudem v Brně, spisová značka B6087
(dále také „dodavatel“)
v návaznosti na výběrové řízení k veřejné zakázce malého rozsahu s názvem **Nástroj pro ochranu elektronické pošty**, evidenční číslo: VZ166519, objednatele uzavírají tuto smlouvu na dodání softwaru a licencí (dále jen „smlouva“)

2. Předmět smlouvy

2.1. Smlouvou se dodavatel zavazuje dodat objednateli software včetně příslušenství nutného k efektivnímu využití softwaru dle specifikace uvedené v příloze č. 1 smlouvy (dále jen „software“).

2.2. Smlouvou se dodavatel dále zavazuje k dodání podkladů potřebných pro používání softwaru, zejména uživatelského manuálu (návodu k obsluze) v českém či anglickém jazyce (v tištěné či elektronické podobě), a k poskytnutí součinnosti objednateli s uvedením softwaru do provozu způsobem a v rozsahu dle přílohy č. 1 smlouvy.

2.3. Smlouvou se dodavatel dále zavazuje k zajištění podpory výrobce softwaru v rozsahu a za podmínek uvedených v příloze č. 1 smlouvy.

2.4. Předmětem smlouvy je dále závazek objednatele za řádně a včas dodaný software a zajištěnou podporu výrobce zaplatit dohodnutou cenu.

3. Doba a místo dodání

3.1. Dodavatel se zavazuje dodat software v rozsahu uvedeném ve smlouvě do 30 dnů od uzavření smlouvy.

3.2. Software bude dodán na Oddělení informatiky Masarykova onkologického ústavu.

4. Předání a převzetí software

4.1. Dodavatel se zavazuje nahlásit minimálně tři dny předem předpokládaný termín dodání osobám dle přílohy č. 3 smlouvy.

4.2. Dodáním software se má na mysli (a) dodání instalačních souborů software a licenčních klíčů nebo (b) zajištění (online) přístupu k instalačním souborům software a dodání licenčních klíčů. Licenčními klíči se mají na mysli licenční klíče, které objednateli umožní nabytí časově neomezených licencí k software.

4.3. Pokud bude nutné provést registraci softwaru dodavatelem, pak ji dodavatel provede na objednatele (správce [redacted], e-mail:[redacted]). Dodavatel se dále zavazuje zaslat objednateli identifikační údaje potřebné k přístupu k licencím (Autorizační číslo a Číslo licence), a to e-mailem na[redacted].

4.4. Objednatel je povinen převzít software, který je dodán řádně, tj. který zejména vykazuje všechny vlastnosti a vyhovuje všem podmínkám uvedeným ve smlouvě či stanoveným objednatelem nebo právními předpisy.

4.5. Objednatel není povinen převzít software zejména v následujících případech:
- software vykazuje vady, které brání jeho řádnému užívání,
- software není dodán v termínu uvedeném ve smlouvě.

4.6. Software se považuje za předaný a převzatý dnem písemného potvrzení dodání softwaru objednatelem dodavateli, ze kterého vyplývá, že objednatel software přebírá.

5. Cena a platební podmínky

5.1. Celková cena softwaru včetně zajištěné podpory softwaru výrobcem softwaru (dále jen „cena“) činí **1 964 500 Kč bez DPH**.

Rozklad ceny dle jednotlivých položek včetně informace o jednotkových cenách a množství jednotlivých položek je uveden v příloze č. 2 smlouvy.

5.2. Cena zahrnuje veškeré náklady dodavatele související s dodáním a instalací softwaru (včetně součinnosti dodavatele dle čl. 2.2. smlouvy, resp. přílohy č. 1 smlouvy) a je stanovena jako konečná a nepřekročitelná.

5.3. Cena bude uhrazena na základě faktury vystavené dodavatelem po převzetí softwaru objednatelem s dobou splatnosti do 30 dnů ode dne doručení faktury objednateli. Daň z přidané hodnoty (dále jen „DPH“) bude dopočítána a uhrazena ve výši dle právních předpisů účinných ke dni uskutečnění zdanitelného plnění.

5.4. Faktura musí splňovat požadavky daňového dokladu a být v souladu s právními předpisy, zejména se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZoDPH“). Na faktuře musí být uveden název veřejné zakázky a její evidenční číslo. Faktura musí obsahovat rozklad ceny dle jednotlivých položek uvedený v příloze č. 2 smlouvy.

5.5. Nebude-li faktura obsahovat náležitosti dle právních předpisů, popř. bude-li obsahovat jiné chyby či nedostatky, je objednatel oprávněn fakturu vrátit, přičemž nová doba splatnosti počíná běžet dnem doručení opravené faktury objednateli.

5.6. Bude-li objednatel k datu uskutečnění zdanitelného plnění či k datu poskytnutí úplaty za něj dle ZoDPH ručit za nezaplacenou DPH (§ 109 ZoDPH) ze strany dodavatele, je oprávněn část ceny odpovídající DPH uhradit přímo na bankovní účet příslušného správce daně. Část ceny odpovídající DPH se v takovém případě považuje za uhrazenou.

6. Další práva a povinnosti smluvních stran

6.1. Dodavatel si je vědom toho, že v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů, je osobou povinnou spolupůsobit při výkonu finanční kontroly. Dodavatel se zavazuje poskytnout kontrolním orgánům při provádění kontroly maximální součinnost. Dodavatel je zároveň povinen zavázat své subdodavatele, aby tito spolupůsobili při provádění kontroly a poskytovali kontrolním orgánům při provádění kontroly maximální součinnost.

6.2. Dodavatel se zavazuje zajistit dodržování pracovněprávních předpisů, zejména zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami, atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a to vůči všem osobám, které se na plnění zakázky podílejí a bez ohledu na to, zda jsou práce na předmětu plnění prováděny bezprostředně dodavatelem či jeho poddodavateli. Nedodržení tohoto závazku je podstatným porušením smlouvy.

7. Odstraňování vad

7.1. Objednatel je v případě vady softwaru povinen vadu dodavateli nahlásit a uvést, jak se projevuje.

7.2. Dodavatel je v případě nahlášení vady softwaru povinen vadu odstranit do 72 hodin od jejího nahlášení.

7.3. Po odstranění vady je dodavatel povinen předat objednateli servisní výkaz, ve kterém bude vymezena dotčená vada, způsob a čas jejího odstranění. Pokud je vada skutečně odstraněna, objednatel servisní výkaz neprodleně potvrdí (podepíše). Vada se považuje za odstraněnou okamžikem uvedeným v servisním výkazu (ze kterého vyplývá, že vada byla odstraněna), pokud tento okamžik není ve výkazu uveden, pak okamžikem potvrzení servisního výkazu objednatelem. V případě, že objednatel nebude s obsahem servisního výkazu souhlasit, je oprávněn vznést k výkazu své připomínky. Dodavatel je povinen se k těmto vyjádřit nejpozději do 2 dnů ode dne jejich doručení. V případě, že dodavatel tyto připomínky akceptuje nebo v případě marného uplynutí uvedené doby, se servisní výkaz považuje za odsouhlasený ve znění připomínek objednatele. V případě, že připomínky objednatele dodavatel neakceptuje, zavazují se smluvní strany vyvinout maximální součinnost, aby došlo ke shodě. Neposkytnutí součinnosti se považuje za podstatné porušení smlouvy.

8. Komunikace a oprávnění pracovníků smluvních stran, řešení sporů

8.1. Veškerá jednání a komunikace mezi smluvními stranami bude probíhat přednostně prostřednictvím osob a kontaktních údajů vymezených v příloze č. 3 smlouvy. V této příloze jsou rovněž vymezena oprávnění těchto osob.

8.2. Smluvní strany se zavazují případné spory související se smlouvou řešit přednostně smírnou cestou. Nedojde-li k vyřešení sporu smírnou cestou, je každá ze smluvních stran oprávněna přistoupit k řešení sporu soudní cestou.

Smluvní strany v souladu s § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, sjednávají jako místně příslušný Městský soud v Brně. Smluvní strany dále sjednávají, že smlouva a veškeré nároky nebo spory vzniklé na jejím základě nebo v souvislosti s ní (včetně mimosmluvních sporů a nároků) se budou řídit českým právem a budou vykládány v souladu s právními předpisy České republiky.

9. Smluvní sankce

9.1. V případě prodlení objednatele s platbou ceny je dodavatel oprávněn po objednateli žádat uhrazení úroku z prodlení ve výši dle nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob.

9.2. V případě prodlení dodavatele s dodáním softwaru je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 500 Kč za každý započatý den prodlení.

9.3. V případě prodlení dodavatele s odstraněním vady softwaru je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 250 Kč za každou započatou hodinu prodlení.

9.4. Dodavatel je povinen uhradit smluvní pokutu objednateli do 10 dnů počítaných ode dne doručení jejího vyúčtování dodavateli.

9.5. Zaplacení výše uvedené smluvní pokuty se nedotýká nároku objednatele na náhradu škody v plné výši.

10. Platnost a účinnost smlouvy, změny smlouvy

10.1. Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“).

10.2. Smluvní strany souhlasí se zveřejněním smlouvy a případných dohod (dodatků), kterými se smlouva doplňuje, mění, nahrazuje nebo ukončuje, a to zejména v registru smluv v souladu se zákonem o registru smluv. Smlouvu v registru smluv uveřejní objednatel, dodavatel správnost uveřejnění do jednoho měsíce od uzavření smlouvy ověří.

10.3. Plnění předmětu smlouvy před účinností smlouvy se považuje za plnění dle smlouvy a práva a povinnosti z něj vzniklé se řídí smlouvou.

10.4. Smlouvu lze změnit výhradně dohodou smluvních stran v písemné formě podepsanou oběma smluvními stranami, přednostně prostřednictvím vzestupně číslovaných dodatků. Výjimkou je změna adresy sídla a kontaktních údajů, v takovém případě postačuje oznámení dotčené smluvní strany doručené v písemné formě druhé smluvní straně, v případě změny adresy sídla spolu s doklady prokazujícími oznamovanou změnu; ke změně smlouvy dochází dnem doručení oznámení druhé smluvní straně.

10.5. Dodavatel je oprávněn převést svoje práva a povinnosti ze smlouvy vyplývající na jinou osobu pouze s písemným souhlasem objednatele.

10.6. Smluvní strany se nad rámec § 576 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), pro případ neplatnosti některého z ustanovení smlouvy či celé smlouvy zavazují, že si poskytnou potřebnou součinnost k uzavření dohody, kterou by dotčené ustanovení, případně celou smlouvu, nahradily tak, aby obsah a účel smlouvy zůstal v nejvyšší možné míře zachován.

10.7. Každá ze smluvních stran je oprávněna od smlouvy odstoupit v případě podstatného porušení smlouvy druhou smluvní stranou. Na straně objednatele se za podstatné porušení smlouvy považuje jeho prodlení s úhradou ceny softwaru přesahující 60 dnů. Na straně dodavatele se za podstatné porušení smlouvy považuje zejména jeho prodlení s řádným dodáním softwaru přesahujícím 30 dnů, prodlení s odstraněním vady licencí přesahující 168 hodin či situace dle čl. 7.3 smlouvy, v ostatních případech je objednatel oprávněn od smlouvy odstoupit v souladu s § 2001 občanského zákoníku.

11. Ostatní ujednání

11.1. Smlouva je vyhotovena ve dvou stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Je-li tato smlouva podepisována elektronicky, každá ze stran obdrží její shodné, elektronicky podepsané vyhotovení.

11.2. V otázkách výslovně neupravených smlouvou se závazky smluvních stran řídí ustanoveními příslušných právních předpisů, zejména občanského zákoníku.

11.3. Součástí smlouvy jsou její příloha č. 1 Specifikace softwaru, příloha č. 2 Rozklad ceny a příloha č. 3 Kontaktní osoby.

11.4. Smluvní strany prohlašují, že si smlouvu před jejím podpisem přečetly a že s jejím obsahem souhlasí, na důkaz výše uvedeného připojují své podpisy.

V Brně dne 04-07-2023

[redacted]

za objednatele
prof. MUDr. Marek Svoboda, Ph.D.
ředitel Masarykova onkologického ústavu

V Brně dne 30-06-2023

za dodavatele
Ing. Vítězslav Mach, člen představenstva
UNIS COMPUTERS, a.s.

Příloha č. 1
Specifikace softwaru

Antispam, mail server	
HW požadavky	ANO/NE
Zařízení ve formě VM appliance v počtu minimálně dvou kusů (minimální počet požadovaný pro funkční zapojení v režimu HA).	ANO
Podporované virtualizační platformy VMware, HyperV, Citrix.	ANO
Funkční požadavky	ANO/NE
Podpora IPv4 i IPv6.	ANO
Podpora režimu vysoké dostupnosti HA.	ANO
Podpora VLAN.	ANO
Možnost nasazení v režimu gateway/MTA a v transparentním režimu, pokud jsou tyto funkce licencovány, požadujeme dodání licence pro oba režimy.	ANO
Architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty. Výkonnostní požadavky (viz níže) musí odpovídat výkonnosti bez využívání emailové fronty.	ANO
Podpora komunikačních protokolů SMTP, SMTPS, IMAP, IMAPS, POP3, POP3S.	ANO
Plnohodnotná správa pomocí web gui (HTTPs) a CLI (SSH).	ANO
Podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do monitorovacího systému.	ANO
Součástí dodávky musí být i specifický MIB soubor výrobce.	ANO
Podpora archivace (např. přístup do archivu pomocí protokolu IMAP).	ANO
Podpora systémové karantény.	ANO
Podpora uživatelské karantény s uživatelsky přívětivým přístupem.	ANO
Podpora opakované kontroly emailu ve chvíli vyzvednutí emailu z karantény.	ANO
Podpora externího úložiště (šifrovaná komunikace, např. SFTP).	ANO
Podpora bezpečnostních nastavení v souladu se zákonem o kybernetické bezpečnosti (podpora DKIM, SPF, DMARC a další).	ANO
Počet chráněných emailových domén min. 50 a počet chráněných emailových schránek min. 1500.	ANO
Minimální požadovaná výkonnost pro email routing: 5000 emailů/hod.	ANO
Minimální požadovaná výkonnost pro AS + AV kontrolu: 5000 emailů/hod.	ANO
Minimální počet událostí pro content ochranu AV 200 událostí za hodinu.	ANO
AntiSpam ochrana výrobcem spravovaná proprietární AS funkcionalita s možností kategorizace emailu, nalezených URL, ochrana typu spam-outbreak (tj opakované dotázání se signaturového server po předdefinované prodlevě), IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza emailů, podpora systémů třetích stran (blacklisty), kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků) s možností detekce a selekce newsletter emailů, podpora funkce tzv. bounce verification, podpora greylistingu.	ANO
Podpora DNSBL a SURBL.	ANO
Možnost definice lokálního slovníku zakázaných slov (email obsahující některé z těchto slov bude vyhodnocen jako spam).	ANO
Reakce na detekovaný spam s možností přidat: tag, hlavičku, přeposlat na jiný SMTP server, přidání BCC, archivace, odmítnutí (reject), zahození (discard), uložení do karantény a možnost přepsání adresy příjemce.	ANO
Možnost limitace SMTP relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů, možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění hlavičky).	ANO

Antivirová ochrana aktualizovaná výrobcem s možností nastavení následné akce.	ANO
Možnost rozšíření řešení o on-premise sandbox plně funkčně integrovaný s emailovou branou (pokud se jedná o sandbox jiného výrobce, musí být tato funkční integrace garantována a podporována ze strany obou výrobců).	ANO
Ochrana před únikem citlivých informací, filtrování příchozích a odchozích typů souboru (minimálně podpora regulárních výrazů a typů souborů v příloze).	ANO
Podpora funkce ochrany před útoky typu DoS, Antispoofing, rate limiting.	ANO
Lokálně udržované hodnocení odesílatelů (vyhodnocování lokálního skóre odesílatelů na základě nedávné aktivity s možností nastavení omezení pro různé úrovně skóre).	ANO
Podpora tzv. "click protection" (URL obsažená v přijímaných emailech jsou přepsána tak, aby byl uživatel po kliknutí přesměrován na emailovou bránu. Ta provede kontrolu přístupu proti aktuální databázi kategorizovaných URL a přístup povolí/zakáže na základě své konfigurace).	ANO
Integrované logování, reporting a monitoring.	ANO
Podpora REST API pro možnost integrace management funkcí do stávající řídící infrastruktury.	ANO
Podpora funkce šifrování přenosu mailové komunikace end-to-end bez nutnosti instalovat sw na pracovní stanice (např. uložení šifrované zprávy lokálně s možností vyzvednout zprávu bezpečným způsobem přes web rozhraní).	ANO
Podpora tzv. neutralizace dokumentů v příloze (odstranění nebezpečných prvků v dokumentu (makra, URL, …) v dokumentech MS Office a PDF, při zachování původního typu dokumentu.	ANO
Automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel a výrobcem udržovaným slovníkem často používaných hesel.	ANO
Možnost rozšíření o integrace s platformou Exchange online (Office365) a to přes nativní Office365 API (Podpora antivirové antispamové kontroly pro tuto službu v reálném čase).	ANO
Požadavky na výkonnost (výkonnostní hodnoty musí být platné pro velikost emailu 100KB a bez využívání fronty).	ANO
Licenční požadavky	
Součástí nabídky a dodávky musí být podpora výrobce a předplatné pro veškeré požadované funkce na dobu 5 let a 24x7 podporu výrobcem.	ANO
Preferujeme licenční model nezávislý na počtu chráněných emailových domén (počet chráněných emailových domén je 50). Pokud jsou tyto parametry licencované, v tom případě požadujeme dodání licence min. pro 50 emailových domén.	ANO
Preferujeme licenční model nezávislý na počtu chráněných emailových schránek (počet chráněných emailových schránek je 1500). Pokud jsou tyto parametry licencované, v tom případě požadujeme dodání licence min. pro 1500 emailových schránek.	ANO
Součástí dodávky musí být podpora systému v režimu 24x7 obsahující služby pro anti-malware ochranu a anti-spam ochranu a to na dobu 5 let.	ANO
Součástí dodávky musí být součinnost / podpora dodavatele při instalaci a konfiguraci v rozsahu 2 MD (Man-day) (viz čl. 2.2. smlouvy). Dodavatel se zavazuje poskytovat součinnost / podporu na e-mailové adrese a tel. čísle uvedeném v příloze č. 3 smlouvy. V případě, že dodavatel nebude schopen vyřešit problém objednatele výše uvedeným způsobem, může být objednatelem přivolán k řešení na místě. Veškeré náklady jsou součástí ceny dle čl. 5.1. smlouvy.	ANO
Dodavatel musí zaručit součinnost při zajišťování souladu s povinnostmi vztahujícími se na zabezpečení osobních údajů dle čl. 32 až 34 GDPR a při posouzení vlivu na ochranu osobních údajů.	ANO

Katalogový list k nabízenému produktu je přiložen v samostatném *.pdf dokumentu.

DATA SHEET

FortiMail™ for Email Security

Powerful, Scalable Email Security Protection Available in an Array of Deployment Models

With best-in-class performance validated by independent testing firms, FortiMail delivers advanced multi-layered protection against the full spectrum of email-borne threats. Powered by FortiGuard Labs threat intelligence and integrated into the Fortinet Security Fabric, FortiMail helps your organization prevent, detect, and respond to email-based threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.

Protection Against Email-borne Threats

Powerful anti-spam and anti-malware are complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, impersonation detection, and other technologies to stop unwanted bulk email, phishing, ransomware, business email compromise, and targeted attacks.

Validated Performance

Fortinet is one of the only email security vendors to consistently prove the efficacy of FortiMail through independent testing. FortiMail earned a AAA rating from SE Labs and a 99.97% Spam Catch Rate from Virus Bulletin.

Fabric-enabled Email Security

FortiMail is integrated with Fortinet products as well as third-party components help you adopt a proactive approach to security by sharing IoCs across a seamless Security Fabric. It also enables advanced and complementary email security protection for Microsoft 365 Exchange through API-level integration.

Powered by FortiGuard Labs

Fortinet FortiMail is powered by threat intelligence and FortiGuard AI-powered Security Services like antivirus, virus outbreak protection, and antispam, from FortiGuard Labs. With visibility across 600,000 customer environments worldwide, FortiGuard Labs is one of the preeminent threat research teams in existence.

We want full control.

Email security solutions for organizations that prefer full control and management over their email security infrastructure.

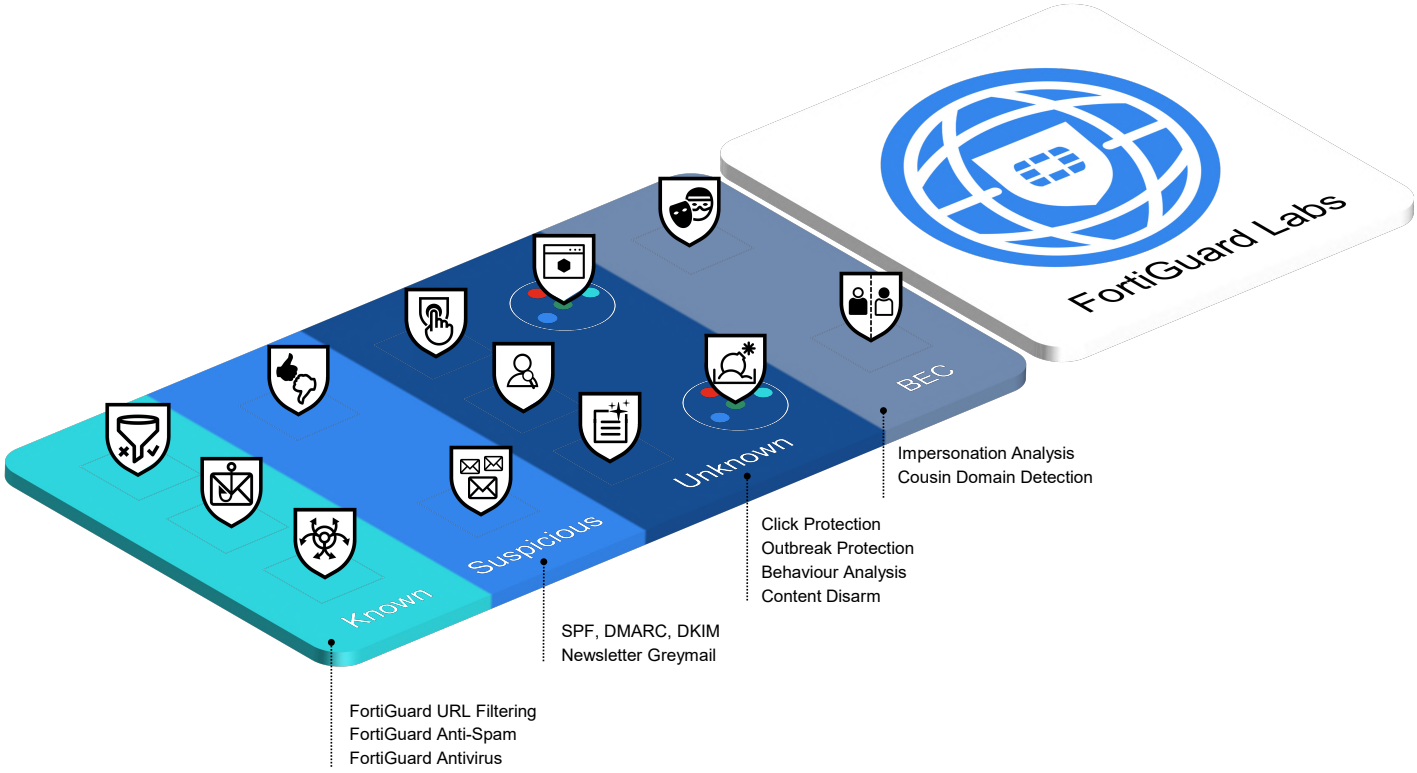
Check the box against:

- ✓ Spam
- ✓ Phishing
- ✓ Spear-phishing and Whale phishing
- ✓ Malicious Attachments and URLs
- ✓ Ransomware
- ✓ Zero-day Threats
- ✓ Impersonation
- ✓ Business Email Compromise (BEC)

FEATURES

Proactive Email Security

FortiMail addresses the full spectrum of risks that email poses to organizations, fortified by FortiGuard Labs' global visibility and intelligence on the latest threats.



Multi-Layered Anti-Spam

Multiple sender, protocol and content inspection techniques shield users from spam and junk mail. Using a combination of reputation analysis, connection filtering, authentication and recipient verification methods allows for fast and accurate email protection. Checks include IP, domain, sender, SPF, DKIM, DMARC and geographical restrictions.

Finally, message structure and content are analyzed based on the digital signature, keywords in context, image analysis, embedded URIs, and more advanced techniques such as behavior analysis and spam outbreak protection. Working together, these techniques consistently identify and block a verified 99.97% of spam in real-world conditions.

Powerful Anti-Malware

Combining multiple static and dynamic technologies that include signature, heuristic, and behavioral techniques along with virus outbreak prevention, FortiMail protects against a wide range of constantly evolving threats.

Advanced Threat Protection

For an even stronger defense against the very latest threat classes like business email compromise and targeted attacks, FortiMail offers optional content disarm and reconstruction, sandbox analysis, sophisticated spoof detection, and more.

Integrated Data Loss Prevention

A robust set of capabilities for data loss prevention and email encryption safely deliver sensitive emails and protect against the inadvertent loss of data. These features facilitate compliance with corporate policies and industry regulations.

Intuitive Controls

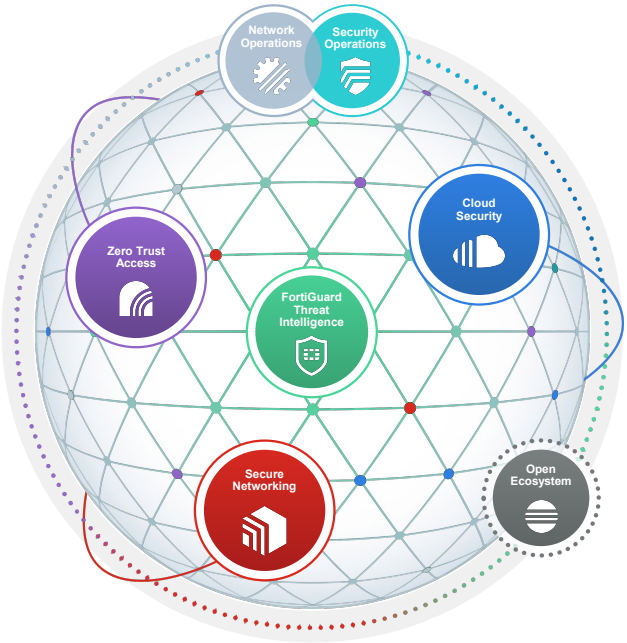
Real-time dashboards, rich reporting, centralized quarantine and simple to use end-user controls allow organizations to get running and realize value quickly. An intuitive user interface combined with flexible MTA and mail-handling capabilities give full visibility and control over email traffic.

FEATURES

Integration with the Fortinet Security Fabric

The future of email security is platform- or fabric-enabled to counter the growing sophistication of threats and multi-vector campaigns. As part of the Fortinet Security Fabric, Indicators of Compromise and other telemetry can be shared for enhanced security across your entire security infrastructure.

IT and security teams are able to more completely connect the dots to identify multi-vector campaigns by sophisticated actors. In addition, intensive and repetitive workflows including response can be automated to reduce the burden on security operations teams.



Industry Recognized, Top-Rated Performance

FortiMail delivers superior performance as measured by independent third-party testers.

99.97%
Spam Catch Rate

100%
Malware Detected

97%
Overall Detection Rate

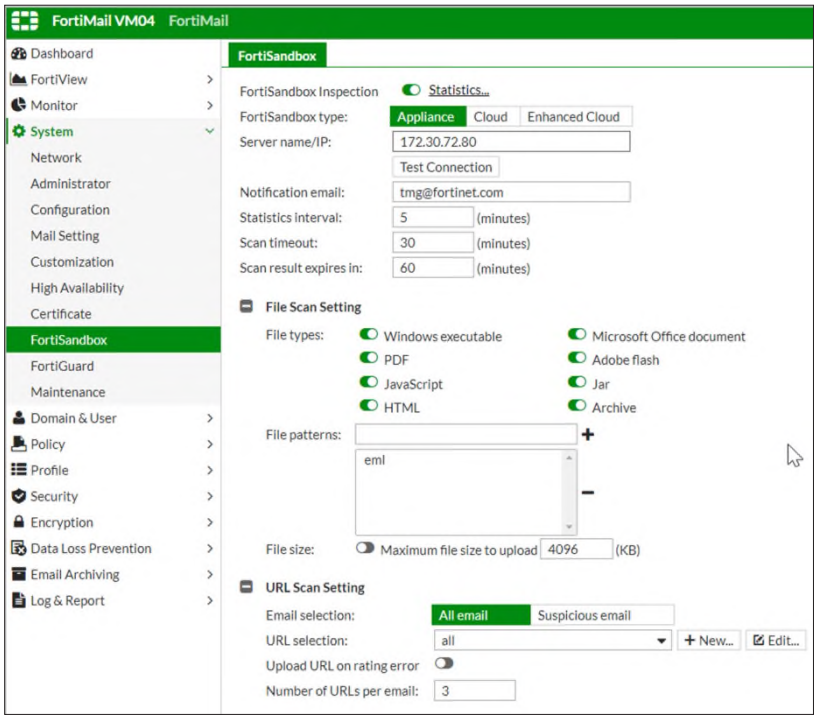
FEATURES

Intuitive Email Management

Real-time dashboards, rich reporting, centralized quarantines, and end user controls along with full MTA and mail-handling capabilities provide organizations full visibility and easy control over email traffic.

Easy-To-Use Configuration

Easy-to-use configuration controls make setting up and managing email security – even advanced security capabilities - easy for organizations of all sizes and use cases.



Hands on or hands off?

Which FortiMail solution is best for you?

We want full control.

Virtual Machines and appliances for teams who want total control over their infrastructure and email security.

Manage it for us.

Email security as a service for teams who just want to focus on monitoring and responding to email threats. Fortinet handles the infrastructure.

Read the FortiMail Cloud data sheet >

FEATURES

High Performance, Flexible Deployment

Scale easily to handle millions of messages per hour. Serving organizations of all sizes, Fortinet provides a wide range of deployment models and operation modes to best match your organization's email security needs.

Deployment Models

Appliances and Virtual Machines

FortiMail appliances and virtual machines are for organizations that prefer full control and management over their email security infrastructure for on-premise and cloud use cases.

- Appliances for on-premise environments
- Virtual machines for running on:
  - Popular hypervisor platforms including:
    - VMWare
    - Citrix XenServer
    - Hyper-V
    - KVM
  - Major cloud platforms:
    - AWS
    - Azure
    - Google Cloud
    - Oracle

FortiMail Cloud

FortiMail Cloud for organizations that want simple, easy-to-use email security as-a-service for both on-premise and cloud-based email services.

Operation Modes

Gateway Mode

Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for analysis. FortiMail then relays safe email to its destination email server for delivery.

Microsoft Graph API Integration

FortiMail can be deployed out of line to simplify deployment, so no MX record change is required, and leverage the native Microsoft 365 API to deliver threat detection and post-delivery message clawback. Broad flexibility is possible with clawback to create policies that address compliance or unique business requirements, such as building search parameters based on keywords, file name, or content type. These capabilities can serve as powerful complements to native Microsoft security features to bolster overall efficacy and reduce risk.

Transparent Mode

Transparent mode eliminates the need to change the DNS MX record, or to change the existing email server network configuration. Transparent mode is particularly appealing for service providers that want to extend email security services to their customer bases. Not available with FortiMail Cloud.

Server Mode

The FortiMail device acts as a standalone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP, and WebMail access.

FEATURES

We want full control.

Feature	Base Bundle	Enterprise Advanced Threat Protection Bundle	Ent. ATP with Microsoft 365 API Support Bundle
99.97% Spam Capture Rate	✓	✓	✓
Advanced Multi-Layer Malware Detection	✓	✓	✓
Inbound and Outbound Filtering	✓	✓	✓
Integration with Customer LDAP	✓	✓	✓
Secure Message Delivery (TLS)	✓	✓	✓
Message Tracking	✓	✓	✓
Virus Outbreak Service	✓	✓	✓
Identity-Based Encryption (IBE)	✓	✓	✓
Reporting	✓	✓	✓
Email Data Loss Prevention	✓	✓	✓
Content Disarm and Reconstruction		✓	✓
URL Click Protection		✓	✓
Impersonation Analysis		✓	✓
Cloud Sandboxing		✓	✓
Real-time Scanning of Microsoft 365 Mailboxes			✓
Scheduled Scanning of Microsoft 365 Mailboxes			✓
Post-delivery Clawback of Newly Discovered Email Threats			✓

Additional Add-on Capabilities

Email Continuity

Email Continuity for FortiMail Cloud is designed to protect valuable productivity by providing emergency mailbox services when organizations experience an outage of their email services.

Dynamic Image Analysis Service

Protects your organization and employees against inappropriate and sexually explicit images.

Integrations with Fortinet Solutions

- FortiAnalyzer
- FortiAnalyzer Cloud
- FortiIsolator
- FortiNDR
- FortiSandbox Cloud
- FortiSIEM
- FortiSOAR

FEATURES SUMMARY

SYSTEM

Wide range of deployment and operation options
– On-premise or public or private cloud deployment
– Gateway, M365 API, Transparent, and Server Mode
– Cloud-Managed Service

Inbound and Outbound Inspection

Support for multiple email domains with per-domain customization
– MSSP multi-tenant support with white label support
– Multi-tier administration

IPv4 and IPv6 Address Support

Virtual Hosting using Source and/or Destination IP Address Pools

SMTP Authentication Support via LDAP, RADIUS, POP3 and IMAP

LDAP-Based Email Routing

Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis

Geographic IP location-based policy

Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management

Mail Queue Management

Multiple Language Support for Webmail and Admin Interface

SMTP RFC Compliance

Modern HTML 5 GUI

Independently tested by SELabs, and Virus Bulletin

Compatibility with cloud services e.g. Microsoft 365, Google Workspace, Amazon AWS, and Microsoft Azure

DNS-based Authentication of Named Entities (DANE) support

ANTISPAM

FortiGuard Antispam Service
– Sender and domain reputation
– Spam and attachment signatures
– Dynamic heuristic rules
– Outbreak protection

Full FortiGuard URL Category Filtering includes
– Spam, malware and phishing URLs
– Pornographic and adult URLs
– Newly registered domains

Greylisting for IPv4, IPv6 addresses and email accounts

Local sender reputation (IPv4, IPv6 and End Point ID-based)

Behavioral analysis

Integration with third-party spam URI and real-time blacklists (SURBL/RBL)

Newsletter (greymail) and suspicious newsletter detection

PDF Scanning and image analysis

Block/safe lists at global, domain, and user levels

Support for enterprise sender identity standards
– Sender Policy Framework (SPF)
– Domain Keys Identified Mail (DKIM)
– Domain-Based Message Authentication (DMARC)

Flexible action and notification profiles

Multiple system and per-user self-service quarantines

TARGETED ATTACK PROTECTION

Content Disarm and Reconstruction
– Neutralize Office and PDF documents (remove macros, active content, attachments, and more)
– Neutralize email HTML content by removing hyperlinks / rewrite URLs

Business Email Compromise (BEC)
– Multi-level anti-spoof protection
– Impersonation analysis — manual and automatic address impersonation detection
– Cousin domain detection

URL Click Protect to rewrite URLs and rescan on access

Integration with FortiIsolator Browser Isolation platform to neutralize browser-based threats

API INTEGRATION

Microsoft 365 Integration
– Post-delivery threat clawback
– Scheduled scan
– Real-time scanning
– Internal mail scanning

CONTENT DETECTION

FortiGuard Antivirus Service detection
– CPRL signature checking
– Heuristic based behavioral detection
– Greyware detection

FortiGuard Virus Outbreak Protection Service
– Global threat intelligence and data analytics

Active content detection (PDF & Office Documents)

Rescan for threats on quarantine release

Custom file hash checking

Mime and file type detection

Comprehensive data-loss prevention with file fingerprinting and sensitive data detection
– Automatic Windows fileshare and manual upload file fingerprinting
– Healthcare, Finance, personally identifiable information and profanity detection

Automatic decryption of Archives, PDF and Office Documents using built-in and administrator-defined password lists and word detection within email body

PDF Scanning and image analysis

Dynamic Image Analysis Service
– Identify and report on illicit and sexually explicit content

ENCRYPTION

Comprehensive encryption support
– Server to server TLS with granular ciphersuite control and optional enforcement
– S/MIME
– Clientless encryption to the recipient desktop using Identity Based Encryption (IBE)
– Optional Outlook plugin to trigger Identity Based Encryption (IBE)

MANAGEMENT, LOGGING, AND REPORTING

Basic/advanced management modes

Per domain, role-based administration accounts

Comprehensive activity, configurations change and incident logging and reporting

Built-in reporting module

Detailed message tracking

Centralized quarantine for large scale deployments

Optional centralized logging and reporting with FortiAnalyzer

SNMP support using standard and private MIB with threshold-based traps

Local or external storage server support, including iSCSI devices

External Syslog support

Open REST API for configuration and management

HIGH AVAILABILITY (HA)

High availability supported in all deployment scenarios
– Active-Passive mode
– Active-Active configuration synchronization mode

Quarantine and mail queue synchronization

Device failure detection and notification

Link status, failover and redundant interface support

ADVANCED

Policy-based e-mail archiving with remote storage options
– Support for Exchange journal archiving

Advanced Email Server feature set including
– Comprehensive webmail interface
– POP3, IMAP mail access
– Calendaring functions
– Undo Send

SAML 2.0 SSO and ADFS integration for webmail and quarantine access

SUPPORT

Simple support options with inclusive bundles

Advanced RMA Support

Professional services and installation support options

SPECIFICATIONS

	FORTIMAIL 200F	FORTIMAIL 400F	FORTIMAIL 900F
Recommended Deployment Scenarios			
	Small businesses, branch offices, and organizations	Small to midsized organizations	Mid to large enterprise, education, and government departments
Hardware Specifications			
10/100/1000 Interfaces (Copper, RJ45)	4	4	4
SFP Gigabit Ethernet Interface	-	-	2
SFP+ 10 Gigabit Ethernet Interface	-	-	-
Redundant Hot Swappable Power Supplies	No	No	Yes
Storage	1× 1TB	2× 1 TB	2× 2 TB (2× 2 TB Optional)
RAID Storage Management	No	Software 0, 1	Hardware 0, 1, 5, 10, Hot Spare (Based on Drive Count)
Form Factor	Rack Mount, 1U	Rack Mount, 1U	Rack Mount, 1U
Trusted Platform Module (TPM)	Yes	Yes	Yes
Power Supply	Single	Single (Dual Optional)	Dual
System Specifications			
Protected Email Domains*	20	100	800
Recipient-based Policies (per Domain / per System) — Incoming or Outgoing	60 / 300	400 / 1500	600 / 2000
Server Mode Mailboxes	150	400	1500
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 400
Data Loss Prevention	No	Yes	Yes
Centralized Quarantine	No	Yes	Yes
Microsoft 365 API Integration	No	Optional	Optional
Performance (Messages/Hour) [Without queuing based on 100 KB message size]			
Email Routing (per hour)**	50 K	250 K	800 K
FortiGuard Antispam + Virus Outbreak (per hour)**	40 K	200 K	500 K
FortiGuard Enterprise ATP (per hour)**	30 K	150 K	400 K
Dimensions			
Height x Width x Length (inches)	1.73 × 17.24 × 16.61	1.73 × 17.24 × 16.38	1.75 × 17.00 × 27.61
Height x Width x Length (mm)	44 × 438 × 422	44 × 438 × 416	44 × 438 × 701
Weight	11.9 lbs (5.4 kg)	25.0 lbs (11.0kg)	33.1 lbs (15.00 kg)
Environment			
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	100V / 3A, 240V / 1.5A	100V / 5A, 240V / 3A	100V / 5A, 240V / 2.5A
Maximum Power Required	62 W	113 W	190 W
Power Consumption (Average)	51 W	77 W	174 W
Heat Dissipation	245 BTU/h	418 BTU/h	681 BTU/h
Forced Airflow	Front to back	Front to back	Front to back
Humidity	5%–90% non-condensing	5%–90% non-condensing	5%–90% non-condensing
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)
Compliance			
	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, RoHS	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS
Certification			
	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant

* Protected Email Domains is the total number of email domains that can be configured on the appliance.
Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.
** Tested using FortiMail 7.0

SPECIFICATIONS

	FORTIMAIL 2000F	FORTIMAIL 3000F
Recommended Deployment Scenarios		
	Large enterprise, education, and government departments	Highest performing appliance for the largest corporate, university, ISP, and carriers
Hardware Specifications		
10/100/1000 Interfaces (Copper, RJ45)	4	4
SFP Gigabit Ethernet Interface	2	2
SFP+ 10 Gigabit Ethernet Interface	-	2
Redundant Hot Swappable Power Supplies	Yes	Yes
Storage	2× 2 TB SAS (6× 2 TB Optional)	2× 2 TB (10× 2 TB Optional)
RAID Storage Management	Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count)	Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count)
Form Factor	Rack Mount, 2U	Rack Mount, 2U
Trusted Platform Module (TPM)	Yes	Yes
Power Supply	Dual	Dual
System Specification		
Protected Email Domains*	1000 / (1500)	2000 / (3000)
Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing	800 / 3000	1500 / 7500
Server Mode Mailboxes	2000	3000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 400	50 / 600
Data Loss Prevention	Yes	Yes
Centralized Quarantine	Yes	Yes
Microsoft 365 API Integration	Optional	Optional
Performance (Messages/Hour) [Without queuing based on 100 KB message size]		
Email Routing (per hour)**	1.6 Million	3.5 Million
FortiGuard Antispam + Virus Outbreak (per hour)**	1.1 Million	2.6 Million
FortiGuard Enterprise ATP (per hour)**	800 K	2.1 Million
Dimensions		
Height x Width x Length (inches)	3.5 × 17.2 × 25.5	3.5 × 17.2 × 25.5
Height x Width x Length (mm)	89 × 437 × 647	89 × 437 × 647
Weight	32 lbs (14.5 kg)	40.0 lbs (18.2 kg)
Environment		
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	10.0A / 110V, 3.5A / 240V	9.8A / 110V, 4.9A / 220V
Maximum Power Required	219 W	379 W
Power Consumption (Average)	189 W	348 W
Heat Dissipation	781 BTU/h	1325 BTU/h
Forced Airflow	Front to back	Front to back
Humidity	8%–90% non-condensing	8%–90% non-condensing
Operating Temperature	41°–95°F (5°–35°C)	50°–95°F (10°–35°C)
Storage Temperature	-40°–140°F (-40°–60°C)	-40°–158°F (-40°–70°C)
Compliance		
	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS
Certification		
	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, NDPP, FIPS 140-2 Compliant

* Protected Email Domains is the total number of email domains that can be configured on the appliance.
Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.
** Tested using FortiMail 7.0

SPECIFICATIONS

TECHNICAL SPECIFICATIONS FOR FORTIMAIL VIRTUAL APPLIANCES	VM01	VM02	VM04	VM08	VM16	VM32
Recommended Deployment Scenarios *						
	Small businesses, branch offices, and organizations	Small to midsized organizations	Mid to large enterprise	Large enterprise	Large enterprise	Large enterprise
Technical Specifications						
Hypervisors Supported	VMWare ESX/ESXi 6.0/6.7/7.0 and later, Citrix XenServer v5.6 SP2/6.0 and later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1 and later, AWS (Amazon Web Services), Nutanix AHV**, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure***					
Maximum Virtual CPUs Supported	1	2	4	8	16	32
Virtual NICs Required (Minimum/Maximum)	1 / 4	1 / 4	1 / 6	1 / 6	1 / 6	1 / 6
Virtual Machine Storage Required (Minimum/Maximum) ****	250 GB / 1 TB	250 GB / 2 TB	250 GB / 4 TB	250 GB / 8 TB	250 GB / 12 TB	250 GB / 24 TB
Virtual Machine Memory Required (Minimum/Maximum)	2 GB / 4 GB	2 GB / 8 GB	4 GB / 16 GB	4 GB / 64 GB	4 GB / 128 GB	4 GB / 128 GB
Performance (Messages/Hour) [Without queuing based on 100 KB message size] *****						
Email Routing	34 K	67 K	306 K	675 K	875 K	1.2 M
FortiGuard Antispam	30 K	54 K	279 K	630 K	817 K	1.1 M
FortiGuard Antispam + Antivirus	26 K	52 K	225 K	585 K	758 K	1.0 M
System Specifications						
Protected Email Domains ******	20	70	500	1000	1500	2000
Recipient-Based Policies (Domain / System) — Incoming or Outgoing	60 /300	400 / 1500	800 / 3000	800 / 3000	1500 / 7500	1500 / 7500
Server Mode Mailboxes	150	400	1500	2000	3000	3000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 400	50 / 400	50 / 600	50 / 600
Data Loss Prevention	No	Yes	Yes	Yes	Yes	Yes
Centralized Quarantine	No	Yes	Yes	Yes	Yes	Yes
Microsoft 365 API Integration	No	Optional	Optional	Optional	Optional	Optional

* Recommended sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric.
If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist.
** FortiMail 7.0.1 has been validated on Nutanix AHV 20201105.2096 and AOS 5.20.1.1.
*** Transparent mode deployment is not fully supported on Microsoft HyperV and cloud hypervisors due to limitations in the available network configurations.
**** For the initial VM setup, 250GB is required to install the default Fortinet OVF file. After deployment, the default OVF file can be deleted and the disk space set no less than 50 GB.
***** Hardware dependent. Indicative figures based on a VMWare 6.0 system utilizing 2x Intel Xeon E5-2620 v4 @ 2.10 GHz restricted to the specified number of cores.
****** Protected Email Domains is the total number of email domains that can be configured on the appliance. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned. Advanced management license increases the protected domain limit by 50%.

ORDER INFORMATION

For information on ordering, please talk with your Fortinet account manager, or refer to the Ordering Guide for a full list of FortiMail-related SKUs and pricing information.

FortiMail Product	SKU	Description
FortiMail 200F	FML-200F	Email Security Appliance — 4x GE RJ45 ports, 1 TB storage
FortiMail 400F	FML-400F	Email Security Appliance — 4x GE RJ45 ports, 2 TB storage
FortiMail 900F	FML-900F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 2000F	FML-2000F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3000F	FML-3000F	Email Security Appliance — 4x GE RJ45 ports, 2× 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail VM		
FortiMail VM01	FML-VM01	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core
FortiMail VM02	FML-VM02	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores
FortiMail VM04	FML-VM04	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores
FortiMail VM08	FML-VM08	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores
FortiMail VM16	FML-VM16	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores
FortiMail VM32	FML-VM32	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores
Accessories		
Power Supply	SP-FAD700-PS	AC power supply for FML-400E
Power Supply	SP-FML900F-PS	AC power supply for FML-400F and FML-900F
Power Supply	SP-FML2000F-PS	AC power supply for FML-2000F
Power Supply	SP-FML3000F-PS	AC power supply for FML-3000F and FML-3200F
Hard Drive	SP-D2TE	2 TB 3.5" SAS hard drive with tray for FML-2000F, FML-3000F and FML-3200F
Hard Drive	SP-FML900F-HDD	2 TB 3.5" SATA hard drive with tray for FML-900F
Service and Support		
Appliances - Hardware plus 24×7 FortiCare and FortiGuard Base Bundle		
Appliances - Hardware plus 24×7 FortiCare and FortiGuard Enterprise ATP Bundle		
Virtual Machines - 24×7 FortiCare and FortiGuard Base Bundle Contract		
Virtual Machines - 24×7 FortiCare and FortiGuard Enterprise ATP Bundle Contract		
Microsoft 365 API Integration Service		
Add-on Capabilities		
Dynamic Adult Image Analysis Service		
Email Continuity		
For Service Providers and Enterprises		
Advanced Administration License for MSSPs and Enterprises requiring multi-tenancy and additional features		

FML-DAT-R57-20221117

Příloha č. 2
Rozklad ceny

Položka	Počet MJ	Cena 1 MJ (Kč bez DPH)	Cena celkem (Kč bez DPH)	Sazba DPH (%)	DPH (Kč)	Cena celkem (Kč vč. DPH)
FortiMail-VM virtual appliance for all supported platforms. 2 x vCPU cores	2,00 ks	192 433,00	384 866,00	21%	80 821,86	465 687,86
5ti letá podpora výrobce softwaru	5 let	307 926,80	1 539 634,00	21%	323 323,14	1 862 957,14
Součinnost / podpora při instalaci a konfiguraci softwaru	2 man day	20 000,00	40 000,00	21%	8 400,00	48 400,00

CENA CELKEM:			1 964 500,00			2 377 045,00

Příloha č. 3
Kontaktní osoby

Objednatel				
Funkce / oblast	**Jméno**	**Pracovní zařazení**	**Telefon**	**E-mail**
Administrativní (zejm. fakturace, smluvní problematika)				
Technická (zejm. dodání softwaru, registrace, reklamace, aktualizace, správa licencí)				
Dodavatel				
Funkce / oblast	**Jméno**	**Pracovní zařazení**	**Telefon**	**E-mail**
Administrativní (zejm. fakturace, smluvní problematika)				
Technická (zejm. dodání softwaru, registrace, reklamace, aktualizace, správa licencí)				
Součinnost / podpora při uvedení softwaru do provozu				