



Financováno
Evropskou unií
NextGenerationEU



NÁRODNÍ
PLÁN OBNOVY

MO
Masarykův
onkologický
ústav

SMLOUVA O DODÁNÍ SOFTWARE

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
zastoupená Ing. Petrem Šulou, předsedou představenstva
IČO: 63476223 DIČ: CZ63476223
bankovní spojení: UniCredit Bank Czech Republic and Slovakia a.s., číslo účtu: 39921026/2700
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, spisová značka B6087
(dále také „dodavatel“)

na základě výběrového řízení k veřejné zakázce malého rozsahu **Nástroj pro dynamickou analýzu souborů (sandbox) [2025]**, evidenční číslo: VZ0224784, zadávané objednatelem a realizované v rámci projektu: Zvýšení kybernetické bezpečnosti v Masarykově onkologickém ústavu, registrační číslo CZ.31.2.0/0.0/0.0/23_095/0008720, (dále jen „projekt“) uzavírají v souladu s § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), tuto smlouvu o dodání softwaru (dále jen „smlouva“):

2. Předmět smlouvy

2.1. Dodavatel se zavazuje dodat objednateli SW Fortisandbox včetně licencí dle specifikace a v rozsahu uvedenými v příloze č. 1 smlouvy (dále jen „software“) a dále se v souvislosti s dodáním softwaru zavazuje k:

- o integraci softwaru s e-mailovou gateway objednatele FortiMail (FML-VM02),
- o dodání všech dokladů a dokumentů potřebných k převzetí a užívání softwaru v souladu s právními předpisy, zejména uživatelských manuálů / návodů k obsluze v českém jazyce v tištěné nebo elektronické podobě,
- o provedení školení správců sítě objednatele v místě plnění nebo on-line formou v českém jazyce v rozsahu dle doporučení výrobce softwaru,
- o zajištění technické podpory výrobce softwaru na dobu alespoň 5 let v režimu „NBD (Next Business Day) on-site“ v rozsahu vymezeném v příloze č. 4 smlouvy.

2.2. Objednatel se zavazuje řádně a včas dodaný software převzít a zaplatit za něj dohodnutou cenu.

3. Doba a místo dodání softwaru

3.1. Dodavatel se zavazuje dodat software a splnit svoje ostatní závazky dle čl. 2.1 smlouvy do 60 dnů od dne nabytí účinnosti smlouvy.

3.2. Dodavatel se zavazuje dodat software v prostorách Masarykova onkologického ústavu (Žlutý kopec 7, 656 53 Brno, Švejdův pavilon).

4. Předání a převzetí softwaru

4.1. Dodavatel písemně oznámí objednateli datum předání softwaru a splnění dalších závazků dle čl. 2.1 smlouvy nejméně 5 pracovních dní předem (nedohodnou-li se smluvní strany jinak, je dodání, předání i převzetí softwaru možné pouze v pracovní dny v době od 8.00 do 15.00 h). Smluvní strany si navzájem potvrdí, případně se domluví jinak.

4.2. Objednatel se zavazuje převzít software, jsou-li závazky dodavatele dle čl. 2.1 smlouvy splněny řádně (zejména je-li software v souladu se smlouvou, právními předpisy a technickými normami; tj. je-li software dodán řádně) a včas, v opačném případě není objednatel povinen software převzít.

4.3. O předání a převzetí softwaru se buďto **(a)** pořídí ve 2 vyhotoveních zápis (dále jen „zápis“) podepsaný zástupci obou smluvních stran obsahující:

- o identifikaci smluvních stran,
- o specifikaci softwaru,

- datum provedení školení k softwaru,
- prohlášení objednatele, zda software převzal (bez výhrad / s výhradami) či nepřevzal,
- datum vyhotovení zápisu,
- pokud objednatel software převezme, je (objednatel) do zápisu povinen uvést:
 - seznam předaných dokladů,
 - vymezení případných vad, se kterými je software převzat (včetně termínů pro jejich odstranění),
- pokud objednatel software nepřevzme, je do zápisu povinen uvést:
 - vymezení důvodů nepřevzetí softwaru.

nebo **(b)** objednatel potvrdí dodací list dodavatele, volba náleží objednateli.

- 4.4.** Smluvní strany obsah zápisu potvrdí podpisy svých zástupců na obou vyhotoveních zápisu, každá smluvní strana obdrží jeden.
- 4.5.** Software se považuje za předané / převzaté okamžikem, ve kterém objednatel podepíše zápis dle čl. 4.3 smlouvy, ze kterého vyplývá, že objednatel software převzal.

5. Odpovědnost za vady, záruka za jakost softwaru, technická podpora výrobce softwaru

- 5.1.** Dodavatel odpovídá za vady, jež má software v době jeho předání.
- 5.2.** Záruka za jakost softwaru se nesjednává.
- 5.3.** Dodavatel se zavazuje sjednat objednateli technickou podporu výrobce softwaru (dále jen „technická podpora výrobce“) v délce 60 měsíců ode dne převzetí softwaru tak, aby objednatel za její poskytování výrobcí softwaru nic nehradil. Cena technické podpory výrobce a odměna za její sjednání jsou zahrnuty v ceně softwaru.
- 5.4.** Technická podpora výrobce musí zahrnovat mj. závazek výrobce softwaru (1) odstranit nahlášenou vadu softwaru v místě dodání nejpozději nejbližšího pracovního dne ode dne nahlášení vady (tzv. „NBD“) a (2) poskytovat aktualizace softwaru. Rozsah technické podpory výrobce a podmínky jejího poskytování jsou blíže vymezeny v příloze č. 4 smlouvy (Technická podpora výrobce).
- 5.5.** Platnost technické podpory výrobce musí být možné ověřit přímo u výrobce softwaru či na jeho stránkách.
- 5.6.** Nesjednání technické podpory výrobce je podstatným porušením smlouvy.

6. Další práva a povinnosti smluvních stran, komunikace a oprávnění pracovníků smluvních stran, řešení sporů

- 6.1.** Dodavatel je povinen splnit své závazky dle čl. 2.1 smlouvy v souladu s právními předpisy a obchodními / licenčními podmínkami výrobce softwaru tak, aby objednatel mohl bez omezení využívat technickou podporu výrobce.
- 6.2.** Dodavatel je oprávněn převést svoje práva a povinnosti ze smlouvy vyplývající na jinou osobu pouze s písemným souhlasem objednatele.
- 6.3.** Dodavatel bere na vědomí, že je v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, osobou povinnou spolupůsobit při výkonu finanční kontroly. Dodavatel se zavazuje poskytnout kontrolním orgánům při provádění kontroly maximální součinnost. Dodavatel se ke stejnému spolupůsobení a poskytování součinnosti kontrolním orgánům zavazuje zavázat rovněž své poddodavatele.
- 6.4.** 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 směny, 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.
- 6.5.** Dodavatel se zavazuje zajistit řádné a včasné plnění finančních závazků svým poddodavatelům. Dodavatel se zavazuje přenést totožnou povinnost do dalších úrovní dodavatelského řetězce a zavázat své poddodavatele k plnění a šíření této povinnosti též do nižších úrovní dodavatelského řetězce. Objednatel je oprávněn požadovat předložení dokladů o provedených platbách poddodavatelům a smlouvy uzavřené mezi dodavatelem a poddodavateli a dodavatel je povinen je bezodkladně poskytnout.
- 6.6.** Dodavatel se zavazuje zajistit, aby byl při plnění smlouvy minimalizován dopad na životní prostředí, a to zejména tříděním odpadu, úsporou energií, a aby byla respektována udržitelnost či možnosti cirkulární ekonomiky.
- 6.7.** Dodavatel prohlašuje, že nebyl ve střetu zájmů dle § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, splnění uvedeného zajistil i u svých poddodavatelů.
- 6.8.** Dodavatel prohlašuje, že splňuje požadavky stanovené v Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, v Rozhodnutí Rady (SZBP) 2022/578 ze dne 8. dubna 2022, kterým se mění rozhodnutí 2014/512/SZBP o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, v Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, a v Rozhodnutí Rady (SZBP) 2022/582 ze dne 8. dubna 2022, kterým se mění rozhodnutí

2014/145/SZBP o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny. Splnění uvedeného zajistil i u svých poddodavatelů.

- 6.9.** Dodavatel bere na vědomí, že objednatel pořizuje software v rámci projektu spolufinancovaného z finančních prostředků EU nebo Státního rozpočtu ČR. Dodavatel bere na vědomí, že jakékoli, byť jen částečné, neplnění jeho povinností vyplývajících ze smlouvy, může ohrozit toto spolufinancování, příp. může vést k udělení sankcí objednateli ze strany orgánů oprávněných k výkonu kontroly projektu.
- 6.10.** Dodavatel bere na vědomí, že je povinen minimálně do konce roku 2036 uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů a poskytovat požadované informace a dokumentaci (včetně účetních dokladů) související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, MZ ČR, Evropské komise, Evropského účetního dvora, OLAF – Evropskému úřadu pro boj proti podvodům, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a že je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout ji při provádění kontroly součinnost.
- 6.11.** Smluvní strany se zavazují, že budou při plnění svých závazků vyplývajících ze smlouvy postupovat v souladu s právními předpisy vztahujícími se k ochraně osobních údajů, zejména v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Dodavatel tímto potvrzuje, že byl v okamžiku získání osobních údajů seznámen objednatel s informacemi o zpracování osobních údajů pro účely splnění práv a povinností dle smlouvy. Bližší informace o zpracování osobních údajů poskytuje objednatel na svých internetových stránkách www.mou.cz v sekci „GDPR a ochrana osobních údajů“.
- 6.12.** 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.
- 6.13.** 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 soud 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.

7. Cena softwaru a platební podmínky

- 7.1.** Celková cena za splnění závazků dodavatele vyplývajících z čl. 2.1 smlouvy (dále jen „cena softwaru“) činí:

Cena bez DPH: 949 996 Kč

DPH (21%): 199 499 Kč

Cena včetně DPH: 1 149 495 Kč

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

- 7.2.** Cena softwaru zahrnuje veškeré náklady dodavatele související se splněním dotčených závazků a je stanovena jako konečná a nepřekročitelná. V případě změny sazby DPH se výše ceny softwaru včetně DPH a vlastní DPH upraví dle právních předpisů účinných ke dni uskutečnění zdanitelného plnění.
- 7.3.** Cena softwaru bude uhrazena na základě faktury vystavené dodavatelem po převzetí softwaru objednatel s dobou splatnosti do 30 dnů ode dne doručení faktury objednateli.
- 7.4.** 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 a evidenční číslo veřejné zakázky a dále název a registrační číslo projektu.
- 7.5.** 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.
- 7.6.** 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 softwaru odpovídající DPH uhradit přímo na bankovní účet příslušného správce daně. Část ceny softwaru odpovídající DPH se v takovém případě považuje za uhrazenou.

8. Smluvní sankce

- 8.1.** Objednatel je za každý započatý den prodlení s úhradou ceny softwaru povinen uhradit dodavateli úrok z prodlení ve výši dle nařízení vlády č. 351/2013 Sb.
- 8.2.** Dodavatel je za každý započatý den prodlení se splněním jeho závazků dle čl. 2.1 smlouvy povinen uhradit objednateli smluvní pokutu 2.000 Kč.
- 8.3.** Dodavatel je povinen uhradit objednateli smluvní pokutu do 10 dnů ode dne doručení jejího vyúčtování dodavateli.
- 8.4.** Zaplacení jakékoli z výše uvedených smluvních pokut se nedotýká nároku objednatel na náhradu škody ve výši přesahující smluvní pokutu.

9. Platnost a účinnost smlouvy, změny smlouvy

- 9.1.** Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti jejím zveřejněním dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“).
- 9.2.** 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.
- 9.3.** Plnění předmětu smlouvy před účinností smlouvy se považuje za plnění dle smlouvy a práva a povinnosti z něj vzniklé se řídí smlouvou.
- 9.4.** 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.
- 9.5.** Smluvní strany se nad rámec § 576 občanského zákoníku 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.
- 9.6.** 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 a situace popsaná v čl. 5.6. smlouvy.

10. Závěrečná ustanovení

- 10.1.** Smlouva je vyhotovena ve dvou stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Je-li smlouva podepisována elektronicky, každá ze stran obdrží její shodné, elektronicky podepsané vyhotovení.
- 10.2.** Nedílnou součástí smlouvy jsou její přílohy:
- Příloha č. 1 – Technická specifikace softwaru,
 - Příloha č. 2 – Rozklad ceny softwaru,
 - Příloha č. 3 – Kontaktní údaje,
 - Příloha č. 4 – Technická podpora výrobce.
- 10.3.** Smluvní strany prohlašují, že si smlouvu před jejím podpisem přečetly a že s jejím obsahem souhlasí.

V Brně dne (dle elektronického podpisu)

V Brně dne (dle elektronického podpisu)

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

za dodavatele:
Ing. Petr Šula
předseda představenstva UNIS COMPUTERS, a.s.

Technická specifikace softwaru

Požadavky:	Splnění	Poznámky
Obecná specifikace		
On-premise systém sloužící k izolaci a důkladné kontrole potenciálně nebezpečných souborů, které mohou obsahovat malware - tzv. Sandboxing využívající pokročilé techniky typu anti-evasion běžící v místě zadavatele. Systém musí být schopen běhu ve virtualizační platformě VMware nebo na vlastním HW podporovaném výrobcem daného systému.	Ano	Fortinet FortiSandbox FSA-VM00, virtuální appliance pro virtualizační platformu VMware
Detailní specifikace		
Min. čtyři instance pro sandboxing souborů pro Windows OS prostředí (včetně všech potřebných licencí s platností po dobu nejméně 5 let).	Ano	4 instance
Min. čtyři instance pro sandboxing souborů pro MS Office prostředí (včetně všech potřebných licencí s platností po dobu nejméně 5 let).	Ano	4 instance
Podpora operačních systémů pro sandboxing: Windows 7, Windows 8, Windows 10 (zde je navíc požadováno, aby výrobce v tomto směru řešení v čase aktualizoval, udržoval a zařazoval nově vydané oficiální verze, zejména musí být zařazen operační systém Windows 11).	Ano	
Podpora clusterování s cílem dosažení vysoké dostupnosti a navýšování výkonosti v budoucnu.	Ano	
Inspekce vzorků založená na vícevrstvé ochraně před škodlivým kódem - kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandboxing (spuštění v reálném operačním systému).	Ano	
Využití umělé inteligence (AI) a strojového učení (ML). Tyto úrovně musí být integrovány a být součástí zařízení a vzájemně spolupracovat.	Ano	
Možnost detailní konfigurace politik pro kontrolu hrozeb s možností kontroly v různých typech OS.	Ano	
Možnost kontroly jednoho souboru v různých operačních systémech souběžně.	Ano	
Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloudová služba.	Ano	
Detekce komunikace s C&C centry.	Ano	
Podpora detekce přístupu na kompromitované URL.	Ano	
Funkce reportingu nalezených problémů (součástí výsledku nesmí být pouze status, jestli se jedná o čistý/škodlivý kód, ale kompletní informace včetně detailního popisu chování, packet capture, a v případě projevu malware také možnost zachycení screenshotu či video záznamu v rámci GUI).	Ano	
Podpora a funkce reportingu v MITRE ATT&CK formátu pro analýzu SoC.	Ano	
Výstupy (reportování) ve standardních formátech (HTML, CSV, PDF, apod.).	Ano	
Podpora kontroly minimálně pro následující aplikace: MS Office, Adobe Acrobat Reader, Adobe Flash Player, Mozilla Firefox, Google Chrome, Java, MS .NET Framework.	Ano	
Podpora kontroly minimálně pro tyto typy obecně spustitelných a multimediálních souborů: .7z, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .iqy, .iso, .jar, .js, .lnk, .msi, .pdf, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .zip.	Ano	
Možnost napojení a integrace na bezpečnostní prvky ochrany mailové komunikace, její doplnění a rozšíření.	Ano	
Možnost příjmu souborů k sandboxingu pomocí API a podpora rozhraní typu ICAP.	Ano	
Automatická aktualizace signaturových databází odhalených hrozeb.	Ano	
Podpora logování na externí logovací systém.	Ano	
Propustnost min. 100 souborů za hodinu při plném využití systému pro sandboxing.	Ano	100 souborů

FortiSandbox and FortiGuard Sandbox Services



The new FortiSandbox is built on an advanced AI engine that defends against new, emerging, evasive, and previously unseen threats in real time.

Highlights

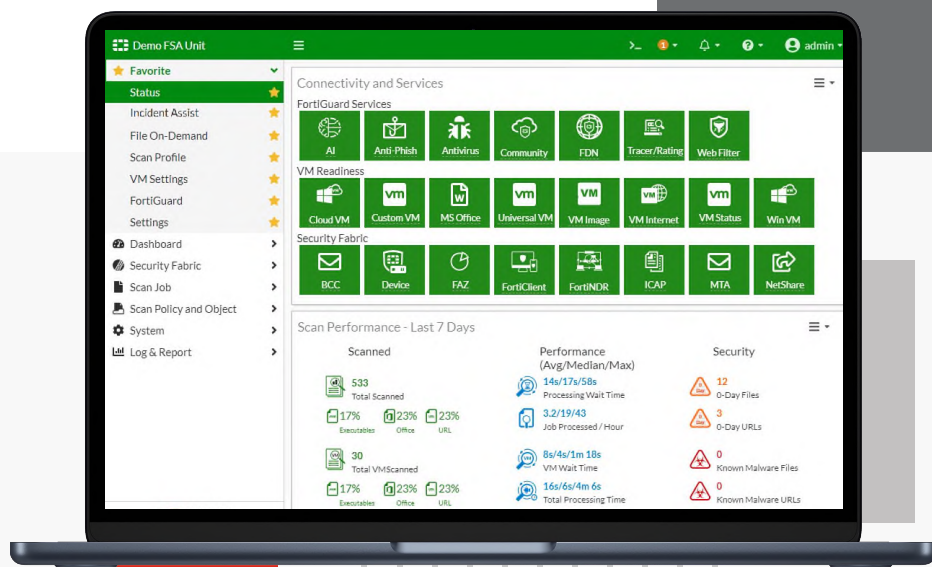
10X Effective Throughput
over traditional Sandboxes, allowing for ultra-scalable operations with no impact on performance

10X Faster Real-Time Verdicts
Accelerate incident handling, increase productivity, reduce exploit windows and reduce downtime and costs while blocking unknown files from entering the network with real-time analysis and filtering

3X Improved Detection and Accuracy
Detect 3X more malware accurately with near-zero false positives

3X More Universal VMs for Scalability and Flexibility
Choose any local, cloud, or custom virtual machine (VM) types and operating systems (OSs)

SOC assistance
FortiSandbox features a single pane of glass view of all threats for analysis and response to assist SOC and IR teams



Next-Level FortiSandbox 5.0: Smarter, Faster, Scalable

FortiSandbox 5.0 is a fast and smart security solution that utilizes a combination of AI/ML, static and dynamic analysis, inline blocking, and scalable virtual environments to identify, analyze, contextualize, prioritize, and protect against advanced threats in real-time. Using an advanced AI engine running on purpose built ML, FortiSandbox 5.0 is 10X faster and offers 3X greater detection and accuracy than before with 3X more universal VMs for expansion than before to protect against malicious activity, including zero-day threats and advanced AI-powered sophisticated threats across a broad attack surface of Cloud, IT, Edge, hybrid, and OT.

FortiSandbox supports multiple operating systems and file types, and provides reporting capabilities for quick threat identification and response. Integrating natively with 12 Security Fabric products and other tools, deployable on-premises, in the cloud, or as a hosted service, FortiSandbox is suitable for organizations of any size.



Defend against the unknown: why sandboxing is mission-critical.

Sandboxing: a must-have in modern cyber defense

As the modern threat landscape, powered by AI enhanced threats bypass traditional defenses, sandboxing has become a critical layer in detecting the unknown and evasive —especially zero-day or fileless malware. This section highlights why sandboxing is no longer optional but an essential and foundational control in modern security strategies.

Framework	Region	Requirement Summary	Primary Industry or Sector
PCI DSS v4.0	 	Mandates anti-malware and recommends advanced techniques (heuristics/behavioral analysis).	Retail, E-commerce, Financial Services, Hospitality, Call Centers
CMMC 2.0		Mandates malware protection.	Defense, Aerospace, Government Contractors
Singapore CCoP		Mandates behavior-based detection (such as sandboxing).	Critical Information Infrastructure (Energy, Water, Finance, Healthcare)
EU NIS2		Mandates risk-based cybersecurity at national level.	Critical Infrastructure, Digital Services, Energy, Telecom
NIST CSF v2.0		Recommends malware detection as an outcome (such as malicious code is detected).	Critical Infrastructure, Government, Finance, Healthcare, Enterprise
Japan METI/IPA		Recommends advanced malware detection (such as sandboxing).	Manufacturing, Technology, Energy, Critical Infrastructure
EU CSA		May require advanced malware detection for high assurance levels and certification.	IT Products and Services (EU Market)

Note: The industry sectors under critical infrastructure are energy, finance, health, telecommunications, transport, and water.



Sandboxing solutions like FortiSandbox offer powerful detection and protection. However, some security team members still have some doubts about the performance of sandboxing. Let's clear the air on that.

Sandboxing isn't slow—it's smarter.

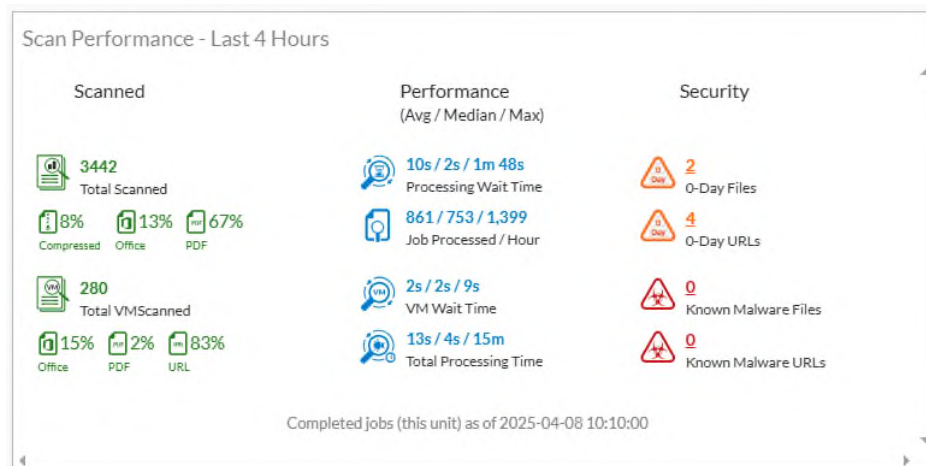
The truth about sandboxing speed

Contrary to outdated beliefs, sandboxing doesn't have to slow things down. FortiSandbox delivers fast, AI-driven threat analysis—proving that high security and high performance can go hand in hand. One of the most common misconceptions about sandboxing is that *it's too slow for real-time protection*. In reality, FortiSandbox is **engineered for speed and efficiency** without compromising on deep threat analysis and protection. It uses a two-tiered AI-powered scanning approach—static and dynamic—to rapidly and accurately assess files.

The Static AI Scan can process up to 50 files per second, immediately identifying known malicious attributes and returning a threat verdict within milliseconds. If a file contains active content (such as embedded URLs, scripts, macros, or executables) but shows no obvious static threats, it is passed to the Dynamic AI Scan, which spins up an isolated virtual environment to detonate and observe the file's behavior—typically within a few seconds.

In a well-resourced production environment, most files are scanned in under a second, with a median scan time of just five seconds. This time-frame is well within acceptable thresholds for network, email, and endpoint solutions to safely hold files during analysis—ensuring high detection efficacy without slowing down operations.

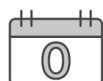
With speed no longer a barrier, it's time to evaluate what really sets sandboxing solutions apart.



The screenshot illustrates the performance of FortiSandbox over the last four hours, highlighting its ability to quickly and efficiently scan a high volume of files and URLs. Over 3000 files and URLs were scanned, with only 8% (280) requiring the more time-intensive Dynamic Scan. The majority of files were processed rapidly, with a median total processing time of just 4 seconds and an average of 13 seconds. Within the efficient scanning process, a handful of suspicious detections were flagged, demonstrating the system ability to balance speed with thorough threat analysis.

A smarter choice: feature-driven evaluation of sandbox technologies

Not all sandboxes are built the same. This section compares key capabilities that matter most—such as AI-driven analysis, deployment flexibility, integration, and automation—to help you choose the right solution for your environment.



Advantage	FortiSandbox	Competitor	Comments
AI/ML Capabilities	✓✓✓	✓✓	FortiSandbox: advanced AI and ML with neural networks available on-premises and cloud, reduce latency. Competitor: AI or ML engine based on cloud-based updates are slower.
Zero-Day Threat Detection	✓✓✓	✓✓	FortiSandbox: Dual analysis (static + dynamic), with fastest Sandbox database creation (e.g. 2 mins) Competitor: High accuracy with rapid signature creation (e.g. 5 mins)
Integration	✓✓✓	✓✓✓	FortiSandbox: Integrates with Fortinet Security Fabric, ICAP, BCC, API. Competitor: Strong integration with their ecosystem.
Deployment Options	✓✓✓	✓✓	FortiSandbox: On-prem, virtual, public-cloud and SaaS cloud. Competitor: Limited selection on-prem, virtual, public-cloud or SaaS cloud.
Forensics Capabilities	✓✓✓	✓✓	FortiSandbox: Full job detailed report. Competitor: Limited to moderate forensic tools.
Automation and Threat Sharing	✓✓✓	✓✓✓	FortiSandbox: Automatic signature distribution. Competitor: Automatic signature distribution.
Cost and Licensing	✓✓✓	✓✓	FortiSandbox: Competitive pricing and simple licensing model. Competitor: Higher tiered pricing and/or per-seat licensing.

Once you understand the features, the next question is: how well does it work across your existing stack?

Better and stronger together: FortiSandbox and the power of coordinated defense

FortiSandbox is designed to integrate deeply across the Fortinet Security Fabric and with third-party products to deliver advanced threat detection and automated response. Here are the most common integrations and use cases.



1. Next-Generation Firewall (NGFW) with Inline Blocking Option

Use Case: Real-time blocking of advanced threats at the network perimeter

When integrated with FortiSandbox, FortiGate NGFW becomes a proactive defense system capable of detecting and blocking sophisticated threats **before they enter the network**. It uses **Inline Scanning**, meaning files and content passing through the firewall (via HTTP, FTP, SMTP) are actively inspected **in real time**.

Suspicious files that cannot be confirmed as safe using static inspection are automatically sent to **FortiSandbox**. If the sandbox determines the file is malicious—through static or dynamic analysis—FortiGate can **immediately block the file**, quarantine the session, or take other actions, all **without delay to users or services**.

With AI-driven detection, high throughput, and tight Security Fabric integration, this setup enables **zero-day threat detection and inline prevention**, offering deep security **without the performance penalty**.



2. Secure Email Gateway (SEG)

Use Case: Prevent phishing, malware, and ransomware via email

Emails with attachments or embedded URLs are scanned through FortiSandbox **to detect hidden malware, phishing and ransomware**. If a threat is confirmed, SEG such as FortiMail can block delivery or strip dangerous content—**stopping email-borne threats before they reach inboxes**.



3. Endpoint Security

Use Case: Endpoint-level detection and response

When Endpoint Security solutions such as FortiClient or FortiEDR, encounter unknown files they forward those to FortiSandbox for analysis. If malware is detected, the endpoint agent can kill the process, isolate the host, or share IOCs with other devices—**creating a fast, coordinated response across users and systems**.

4. Web Proxy



Use Case: Block advanced web threats from downloads and scripts

Proxy devices such as FortiProxy filter web traffic and enforce policies, while FortiSandbox adds deep analysis for suspicious downloads and web content. Together, they detect and block zero-day malware, drive-by downloads, and malicious scripts—**before they ever reach the endpoint**.

5. Shared Storage



Use Case: Analyze files from SMB/NFS shares, cloud storage (e.g. OneDrive), and web uploads

FortiSandbox can scan files from shared folders and upload portals—including SMB, NFS, public shares, and cloud storage like OneDrive. By detecting hidden malware in these locations, it helps **stop lateral movement and insider threats** before they spread.

6. FortiAnalyzer and FortiSIEM



Use Case: Centralized visibility, correlation, and automated response

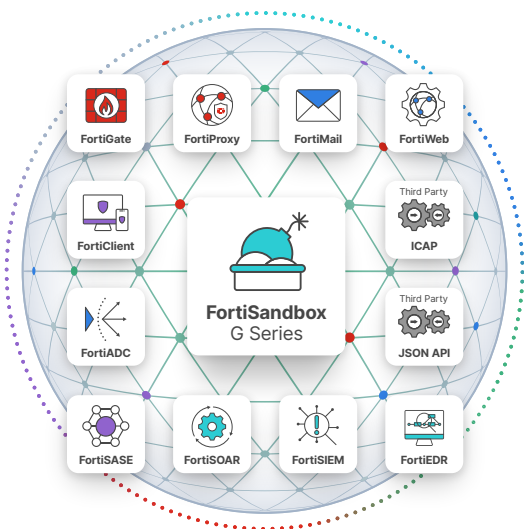
FortiSandbox shares IOCs and threat intelligence with FortiAnalyzer and FortiSIEM. These platforms correlate events, generate alerts, and trigger workflows—**accelerating detection, triage, and mitigation across the enterprise**.

7. Third Party Integrations (via APIs or ICAP)



Use Case: Extend sandboxing to external products

FortiSandbox supports **ICAP** and **RESTful APIs**, allowing integration with third-party tools like other NGFWs, proxies, SIEMs, or email gateways. This integration enables **sandbox-as-a-service** functionality even outside of Fortinet environments.



FortiSandbox doesn't work in isolation—it integrates deeply across the Fortinet Security Fabric. From firewalls and email to endpoints and storage, see how FortiSandbox delivers maximum threat coverage and protection through intelligent and coordinated defense in real-time.

Now that we've explored the value of sandboxing, addressed common misconceptions, and reviewed real-world use cases, it's time to look under the hood. The following section outlines FortiSandbox's core capabilities and technical specifications—highlighting the features that drive its speed, accuracy, and seamless integration across your security infrastructure.

Feature Summary

FortiSandbox combines advanced threat detection with performance and flexibility, making it a powerful addition to any security stack. This section summarizes key features that define its effectiveness—from AI-driven static and dynamic analysis to flexible deployment models and seamless integration across network, endpoint, email, and cloud environments. Whether you're looking for speed, scalability, or automated response, FortiSandbox delivers where it matters most.

Advanced AI Engine

With FortiSandbox 5.0 we have integrated the power of AI/ML directly into the platform. This advanced AI engine with purpose built ML allows FortiSandbox to detect, analyze, and protect against all types of malicious content faster, in real-time without any latency/delays so that organizations are protected against new and emerging threats without adding more resources or cybersecurity controls.

Real-Time Anti-Phishing

The FortiSandbox provides protection against zero-day phishing. The URLs extracted from emails and embedded from documents are processed in the FortiGuard cloud. The web pages are downloaded in real-time and are analyzed using patented technologies to determine any phishing signs.

Incident Assist for Threat Investigation with MITRE ATT&CK-based Reporting and Tools

FortiSandbox provides a comprehensive Job Detail Report for threat analysis and intelligence for Virtual Security Analyst. The report maps discovered malware techniques to MITRE ATT&CK framework with built-in powerful investigative tools that allow Security Operations (SecOps) teams to download captured packets, original file, tracer log, and malware screenshot. STIX 2.0 compliant IOCs provide rich threat intelligence and actionable insight after files are examined.

FortiSandbox also allows SecOps teams to optionally record a video or interact with the malware in a simulated environment.

Universal VM

Universal VM is an all-in-one license for the flexibility to choose any local, cloud, or custom virtual machine (VM) type and operating system. It detaches VM licenses from the OS licenses to reduce licensing complexity.

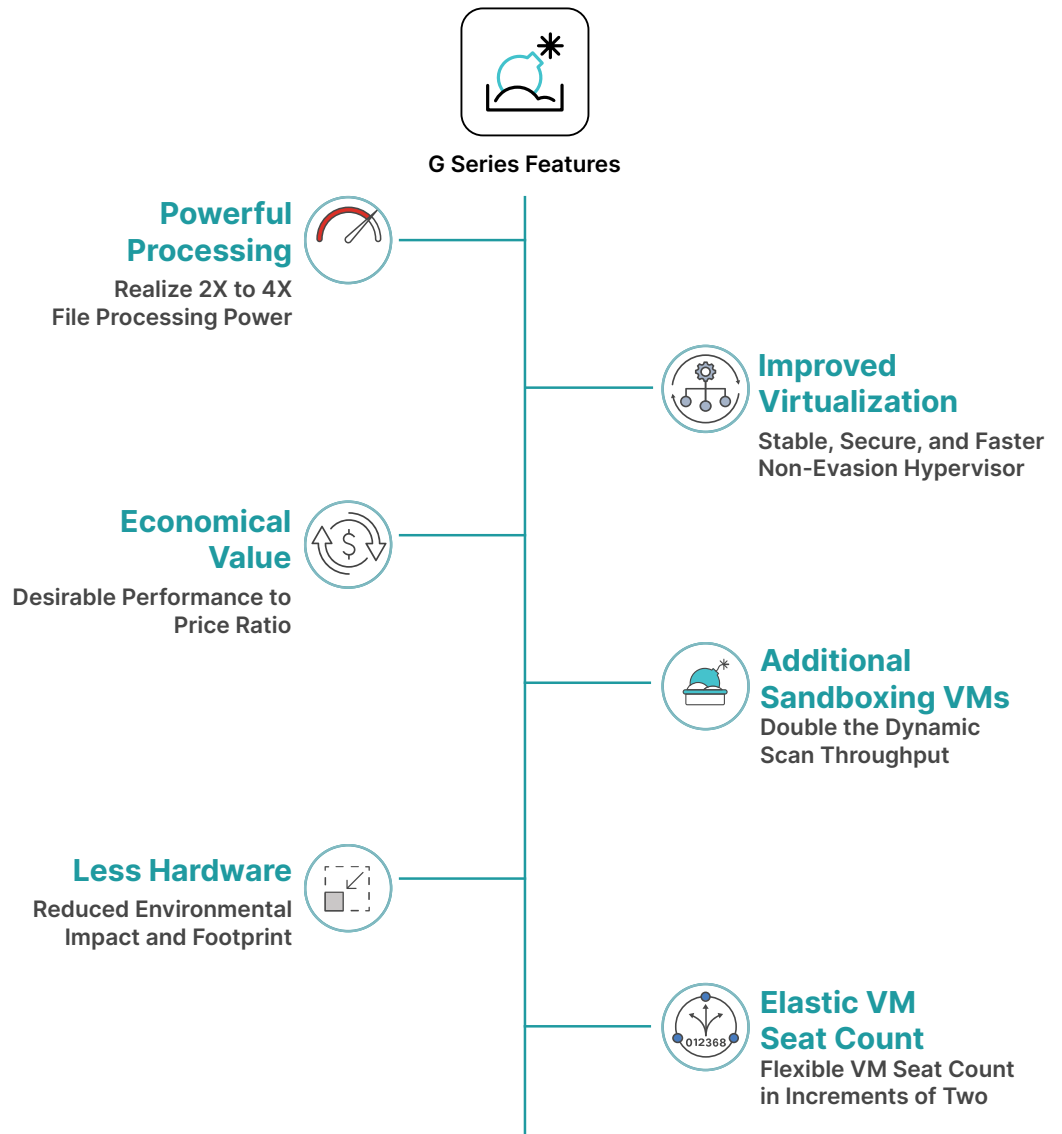
HA-Cluster

The FortiSandbox provides native clustering support of up to 99 worker nodes that expands throughput capacity providing uninterrupted critical operations.



Platform Evolution

Leveraging our previous F and E models*, FortiSandbox 3000G, 1500G, and 500G provide cutting edge technological advancements, performance, real-time sharing of threat intelligence across multiple geographical locations, and integration with Fortinet's Security Fabric and third party providers. With twice the VM capacity and file processing capabilities, our G Series delivers unparalleled stability, the highest detection accuracy, and best-in-breed throughput, while offering flexible and cost-effective deployment solutions.



*The 500G replaces the 500F, and the 1500G replaces the 1000F and 2000E.

Detailed Summary



Advanced Threat Protection

- Advanced AI to identify zero-day threats faster and better detection
- Inline blocking to detect and protect against Zero-day Malware including ransomware; blocks and holds malicious content at the FortiGate and sends to the sandbox for analysis/verdict
- Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- Threat enrichment through FortiGuard IOC
- Sandbox Community Cloud for shared analysis within the worldwide community of FortiSandbox deployments



System Integration Support

- File and URL submission by Security Fabric devices
 - Integrated mode with FortiGate. HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM, and their equivalent SSL-encrypted versions
 - Integrated mode with FortiMail. SMTP, POP3, IMAP
 - Integrated mode with FortiClient EMS. HTTP, FTP, SMB
 - Integrated mode with FortiWeb. HTTP
- Sniffer mode. HTTP, FTP, POP3, IMAP, SMTP, SMB
- Proxy inspection via ICAP
- MTA/BCC mode via SMTP
- NetShare Scan mode via FTP, sFTP, CIFS, NFS, OneDrive, AWS S3 Buckets, Azure Blob, and Google Cloud storage.
- Dynamic Threat Intelligence DB update of malicious file checksum and URL
- JSON API to automate uploading samples and downloading actionable malware indicators to remediate
- Remote and secured logging with FortiAnalyzer, FortiSIEM, CEF servers, and syslog servers



Deployment

- File submission from integrated device(s)
- Sniffer mode deployment with TCP RST support to reset client's connection with the suspicious server
- Network Share Scan with large file support (e.g., ISO images, network shared folders, SMB/ NFS, AWS S3, and Azure Blob)
- Proxy adapter submission with multi-tenancy support
- OT deployment with supported services: BACnet, HTTP, IPMI, Modbus, S7comm, SNMP, TFTP
- High-availability with Primary and Secondary nodes for redundancy
- Port monitoring for cluster fail-over
- Clustering up to 99 worker nodes for higher throughput
- Air-gapped networks support
- Aggregate interface support for increased bandwidth and redundancy
- Isolated administrative traffic from VM image traffic



Detailed Summary continued



Advanced AI Scan (Static AI Scan) Features

- Integrated with the new Advanced AI engine and model
- Integrated with the full FortiGuard Antivirus database of heuristic and checksum signatures
- Intelligent adaptive scan profile that optimizes sandbox resources based on submissions
- Parallel scan to run multiple distinct VM types simultaneously
- Extracts and scan files embedded in documents
- Extracts and scan URLs embedded in documents and QR Code
- Extracts and scan images in documents using OCR
- Integrate with third-party Yara rules
- Cloud query for latest known Malware and clean files
- File checksum whitelist and blacklist options
- Scan URLs from submitted emails and files
- Rating Engine Plus that leverages the latest FortiGuard ML rating
- VM scan ratio for efficient utilization of VMs



Sandboxing VM (Dynamic AI Scan) Support

- AI-powered behavioral analysis constantly learning new malware and ransomware techniques
- Concurrent dynamic analysis VM instances
- OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems
- Customizable VMs for Windows and Linux OS
- Configurable internet browser supporting Internet Explorer, Microsoft Edge, Google Chrome, and Mozilla Firefox
- Sandbox interactive mode, video-recording of malware interaction and VM screenshots
- Nested VMs on premise and cloud deployment
- Anti-evasion detection techniques
 - API Obfuscation
 - Bare-metal Detection
 - Command and Control
 - Direct System Calls
 - Execution Delay
 - Memory Only Payload
 - Process Hollowing/Injection
 - Runtime Encryption/Packing
 - System Fingerprinting
 - Time Bomb
 - User Files Check
 - User Interaction Check
 - VM/Sandbox Detection
- Callback detection. Malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
- Downloadable captured packets, tracer logs, and screenshots
- File Types Support: Windows Executable, Microsoft Office, Document/Email, Android files, Linux files, MacOS, Web files
- File Compression Support: 7z, ace*, arj, bz2, gz*, iso*, jar, .kgb*, lzh, rar, swf*, tar, tgz*, udf, upx*, vhd*, xz, z*, zip (* not supported in SaaS yet)
- User-defined extensions



Detailed Summary continued

Monitoring and Reporting



- AI-based Threat Summary using the collected indicators and results
- Dashboard widgets for connectivity and services, license status, scan performance, system resources
- Scan performance page for tracking historical usage
- Real-time monitoring widgets. Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious URLs, top callback domains
- Drilldown event viewer. Dynamic table including actions, malware name, rating, type, source, destination, detection time, and download path
- Reports and logging. GUI, download PDF, and raw log file
- Detailed Job Report generation
- Periodic logs of system status, performance, scan statistics, and system resource usage
- MITRE ATT&CK v11 support
- Download tracer logs, PCAP, and indicators in STIX 2.0 format
- Notification emails when a malicious file is detected
- Weekly reports to global email lists and administrators
- TAC-report for comprehensive snapshot of system configuration and status

Administration



- Configuration via GUI and CLI
- Multiple administrator accounts supporting full or view only access
- Radius authentication for administrators
- Single Sign-On via SAML
- Self-Check widget for configurations, connectivity, and services
- Cluster management page for administering the HA and cluster nodes
- Centralized search page allowing administrators to build customized search conditions
- Upload any license from a single convenient page
- VM status monitoring
- Automatic engine and signature updates
- Automatic check for new VM image availability
- System health check alerting system
- NTP via FortiGuard support
- Backup, restore, and revision of system configuration
- Consolidated CLI for troubleshooting
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option on NetShare scan mode to prioritize and forward files to a third-party scanning for further scanning

Deployment and Detection Specifications

FEATURE	CLOUD			ON PREMISE		
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VMs	FSA Hardware
Deployment and Integration						
Type						
Deployment	Fortinet Hosted	Fortinet Hosted	Fortinet Hosted	Azure, AWS, GCP, OCI	On Premise	On Premise
Hosting	Shared	Shared	Dedicated	Dedicated	Dedicated	Dedicated
Integration						
Security Fabric	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partner	—	—	✓	✓	✓	✓
API, BCC, ICAP, MTA, NetShare, and Sniffer Mode	—	—	only API	✓	✓	✓
FortiGate Capabilities						
Detection (Visibility and Log Enrichment)	✓	✓	✓	✓	✓	✓
Prevention (Inline Blocking)	—	✓	✓	✓	✓	✓
Detection						
Static Analysis						
Advanced AI ¹				✓ ¹	✓ ¹	✓ ¹
Static AI Engine ³	✓	✓	✓	✓	✓	✓
Accelerated AI Pre-filter ²		✓	Add-on	Add-on	Add-on	Add-on
Antivirus Extended DB	✓	✓	✓	✓	✓	✓
Web Filtering	✓	✓	✓	✓	✓	✓
Dynamic Analysis						
Dynamic AI Engine ³	✓	✓	✓	✓	✓	✓
Analysis Time	up to 60 mins	1-5 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes
Universal VM ⁴				✓	✓	✓
Real-Time Anti-Phishing			Add-on	✓ ¹	✓ ¹	✓ ¹
Anti-Evasion Detection	✓	✓	✓	✓	✓	✓
IPS and C&C Detection	✓	✓	✓	✓	✓	✓
Supported OS						
Windows	✓	✓	✓	✓	✓	✓
MacOS, Linux, Android	—	✓ ⁵	✓ ⁵	✓	✓	✓
Custom VM	—	—	—	✓	✓	✓
OT Simulation	—	—	—	✓	✓	✓

1. Available as part of "Advanced Sandbox Threat Intelligence" subscription running on firmware version 5.0.

2. Add-on integration with FortiNDR appliance for fast pre-filtering.

3. AI-powered content and behavioral analysis through Machine Learning Model updated via Sandbox Threat Intelligence subscription.

4. Supported on firmware version 5.0.

5. Dynamic Scan on Android is scheduled for 2025/Q3.



Supported File Type Specifications

FEATURE	CLOUD			ON PREMISE		
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VMs	FSA Hardware
Supported File Type						
Windows Executables						
Portable executable and batch files (exe, bat)	✓	✓	✓	✓	✓	✓
Additional format (cmd, dll, msi, jar, ps1, scr, vbs, wsf)	—	—	✓	✓	✓	✓
Productivity Files						
Microsoft Office (Word, Excel, Powerpoint, Publisher)	✓	✓	✓	✓	✓	✓
Portable document format files (pdf)	✓	✓	✓	✓	✓	✓
Other related files (csv, ics, rtf)	—	—	✓	✓	✓	✓
Email						
Email files (eml)	—	—	✓	✓	✓	✓
Links contained in emails (lnk)	—	—	✓	✓	✓	✓
Script-based files						
Windows script files (bat, hta, js, ps1, vbs)	—	—	✓	✓	✓	✓
Web files						
Common files (asp, hta, htm, html, js, lnk, url)	—	—	✓	✓	✓	✓
Adobe Flash files (swf)	—	—	✓	✓	✓	✓
Images						
Images with QR Code and Ransomware	—	—	✓	✓	✓	✓
Additional OS						
Android application package files (apk)	—	✓ ¹	✓ ¹	✓	✓	✓
Linux and Shell scripts files (elf, sh)	—	✓	✓	✓	✓	✓
MacOS files (dmg)	—	✓	✓	✓	✓	✓
Archive Common files						
Common files (7z, arj, cab, bz2, bzip, gzip, lzw, rar, tar, lzh, zip, xz)	✓	✓	✓	✓	✓	✓
Additional Archive files (ace, gz, iso, kgb, swf, tgz, udf, upx, vhd, z)	—	—	✓	✓	✓	✓

1. Dynamic Scan on Android is scheduled for 2025/Q3.



Capacity and Performance Specifications

FEATURE	FSA-PaaS	FSA-VMS1	FSA-VMS2	FSA-VMS3	FSA-VMS4 ⁹	FSA-500G	FSA-1500G	FSA-3000G
Capacity								
Local VM Capacity		0-8	0-16	0-32	0-64	2-14	2-28	8-150
Cloud VM Expansion ¹	1-200	1-200	1-200	1-200	1-200	1-80	1-120	1-200
Performance and Capacity								
Effective Sandboxing Throughput ² (Files/Hr)	5000 ³	8000 ⁴	24 000	48 000	96 000	10 000	32 000	160 000
Static Analysis Throughput ⁵ (Files/Hr)	10 000 ³	20 000 ⁴	60 000	120 000	240 000	20 000	80 000	320 000
Dynamic Analysis Throughput ⁶ (Files/Hr)	160 ³	200 ⁴	400	800	—	500	1000	5700
FortiMail Throughput ⁷ (Emails/Hr)	50 000	80 000	240 000	480 000	960 000	100 000	320 000	1 600 000
MTA Adapter Throughput (Emails/Hr)	—	20 000	60 000	120 000	240 000	25 000	80 000	320 000
Sniffer Mode Throughput (Gbps)	—	1	TBD	TBD	TBD	0.5	4	9.6
Number of Users ⁸	650	1000	3000	6000	12 000	1250	4000	20 000

Notes:

The FSA VMS is tested on premise Hyper-V server with corresponding CPUs, memory, and VMs.

The FSA Public Cloud BYOL could achieve similar performance based on chosen resources.

The performance of FSA SaaS, FSA IL MPS and FSA Public Cloud PAYG are not included, as they cannot be accurately measured.

1. The ranges reflect Universal VM support through firmware version 5.0.
2. Tested based on files with 80% documents and 20% executables; measured based on v5.0. Includes both static and dynamic analysis with pre-filtering enabled.
3. Tested on default Flavor-1 VM (with 4 CPUs and 8GB RAM) and 8 VMs. A higher VM flavor can be provided with 20 or more VM subscriptions for higher capacity. To inquire about VM flavors contact your account representative.
4. Tested on a Hyper-V (with 16 CPUs and 32GB RAM) and 8 VMs.
5. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v5.0.
6. Tested with Static Analysis and all files are forwarded to Dynamic Analysis.
7. Based on a ratio of one email with attachment to 10 emails.
8. Based on a ratio of one user per 80 emails on 10 hour period with 10% on Dynamic Scan.
9. Throughput is constrained by the 96 vCPU limit in version 5.0.



Hardware Specifications

FEATURE	FSA 500G	FSA 1500G	FSA 3000G
System Information			
Form Factor	1RU Appliance	1RU Appliance	2RU Appliance
Network Interfaces	4x GE RJ45 ports	4x GE RJ45 ports, 2× 10 GE SFP+ slots	8× 10 GE SFP+ slots
Storage	1× 960 GB	2× 960 GB RAID1	4× 2 TB RAID-10
Hot Swappable	—	✓	✓
Trusted Platform Module (TPM)	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	1.73×17.24×14.96	1.73×17.24×24.02	3.5×17.2×25.6
Height x Width x Length (mm)	44×438×380	44×438×610	88×438×650
Weight (lbs/kg)	11.42 lbs (5.18 kg)	24.92 lbs (11.30 kg)	44 lbs (20 kg)
Power			
Number of Power Supplies	1x	2x	2x
Power Supply (AC/DC)	100–240V AC 50/60 Hz	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz
Maximum Current (AC/DC)	100V/6A, 240V/3A	100V/7.5A, 240V/3.9A	100V/10A, 240V/5A
Power Consumption (Average/Maximum)	71.8 W / 87.8 W	238.1 W / 291.06 W	471.9 W / 542.4 W
Redundancy	—	✓	✓
Hot Swappable	—	✓	✓
Environment			
Forced Airflow	Front to Back	Front to Back	Front to Back
Heat Dissipation	333.63 BTU/h	1027.22 BTU/h	1850.67 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-20°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	10% to 90% non-condensing	10% to 90% non-condensing	10% to 90% (non-condensing)
Compliance			
Certifications	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST		
Additional Services			
24 × 7 Support	✓	✓	✓



FortiSandbox 500G



FortiSandbox 1500G



FortiSandbox 3000G

Integration Matrix

Product	CLOUD				APPLIANCES
	SaaS	Inline Sandbox	FortiSandbox Cloud (PaaS)	Private/Public Cloud	VM / Hardware
FORTIGATE	FortiOS V7.0+	FortiOS V7.2.1+, FortiOS V7.4.1+ (PaaS)	FortiOS V7.0+		FortiOS V7.0+
FORTICLIENT	FortiClient for Windows OS V7.0+		FortiClient for Windows OS V7.0+		FortiClient for Windows OS V7.0+
FORTIMAIL	FortiMail OS V6.2+		FortiMail V7.0+		FortiMail OS V7.0+
FORTIWEB	FortiWeb OS V7.0+				FortiWeb OS V7.0+
FORTIADC	FortiADC OS v6.0+				FortiADC OS V7.0+
FORTIPROXY	FortiProxy OS v7.0+ FortiProxy OS v7.4+				FortiProxy OS V7.0+

Ordering Information

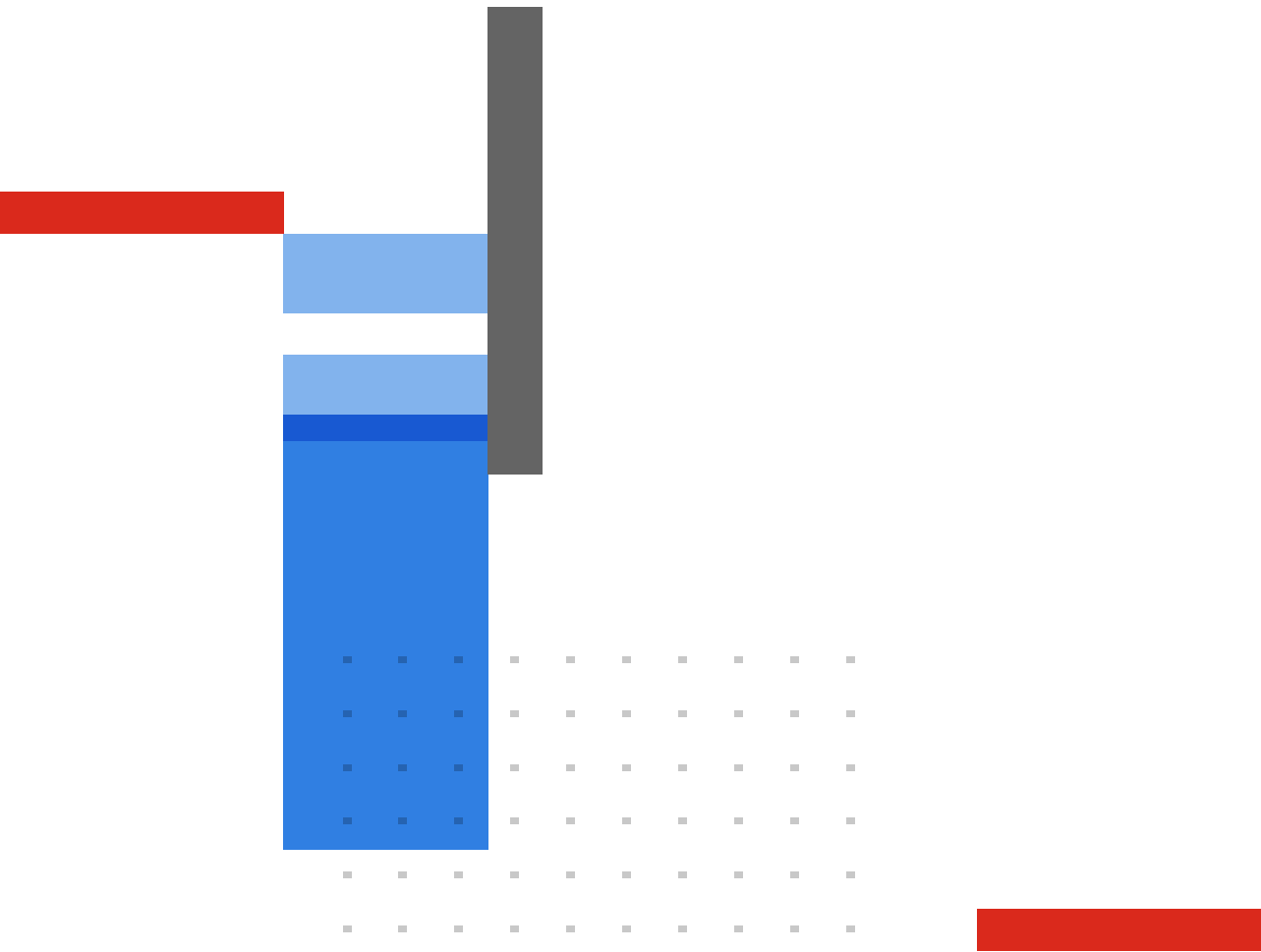
The following SKU list outlines the primary Sandbox deployment options. For full guidance, please refer to the related ordering guides at <https://www.fortinet.com/resources/ordering-guides>.

Product	SKU	Description
FortiSandbox SaaS for FortiGate		
Enterprise Protection (includes IL MPS) (FGT-60F)	FC-10-0060F-809-02-DD	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)
Inline Malware Prevention Service (IL MPS) (a la carte SKU) (FGT-60F)	FC-10-0060F-577-02-DD	FortiGuard AI-based Inline Malware Prevention Service. (Also available as part of the Enterprise Bundle)
Cloud Sandbox (FGT-60F)	FC-10-0060F-100-02-DD	Advanced Malware Protection (AMP) Bundle including Antivirus, Mobile Malware and FortiGate Cloud Sandbox Service.
FortiSandbox SaaS for Security Fabric		
Cloud Sandbox for FortiMail (FML-200F)	FC-10-FE2HF-123-02-DD	FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail.
Cloud Sandbox for FortiWeb (FWB-100E)	FC-10-W01HE-123-02-DD	FortiWeb Cloud Sandbox - Cloud Sandbox for FortiWeb.
Cloud Sandbox for FortiProxy (FPX-400E)	FC1-10-XY400-514-02-DD	SWG Protection Bundle which includes Sandbox Cloud.
Cloud Sandbox for FortiADC (FAD-220F)	FC-10-AD2AF-123-02-DD	FortiADC Cloud Sandbox - Cloud Sandbox for FortiADC.
FortiSandbox PaaS		
FortiSandbox Cloud 1 VM	FC1-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VM for Windows/macOS/Linux/Android by one. (Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD.)
FortiSandbox Cloud 5 VMs	FC2-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VMs for Windows/MacOS/Linux/Android by five. (Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD.)
FortiCloud Premium Account License	FC-15-CLDPS-219-02-DD	Access to advanced account and platform features. Per account license. (See FortiCloud datasheet for included feature and license details.)
FortiSandbox Pub Cloud / FortiSandbox VM Appliance		
FortiSandbox-VMS	FSA-VMS	Subscription license for FortiSandbox-VM with Advanced AI bundle, supporting 16 vCPUs and expandable up to 8 Universal VMs.
FortiSandbox On Premise Hardware		
FortiSandbox 500G	FSA-500G	Sandboxing Hardware Appliance for SMB. Includes two Universal VM count. Available VM count expansion up to max 14 Local and 80 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses.
FortiSandbox 1500G	FSA-1500G	Sandboxing Hardware Appliance for Mid-Range. Includes two Universal VM count. Available VM count expansion up to max 28 Local and 120 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses.
FortiSandbox 3000G	FSA-3000G	Sandboxing Hardware Appliance for Enterprise. Includes eight Universal VM count. Available VM count expansion up to max 150 Local and 200 Cloud. Includes 4xWin10, 4xWin11, 1xOffice21 Licenses.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Příloha č. 2

Rozklad ceny softwaru

Položka	MJ	Počet MJ	Cena za 1 MJ (Kč bez DPH)	Cena celkem (Kč bez DPH)
FSA-VM00 Sandboxing Virtual Appliance. Available Universal VM expansion supports up to max 8 local and 200 cloud, with a total count not exceeding 200. No Universal VM count and Microsoft licenses included. [dodávka softwaru]	ks	1	211 549,00 Kč	211 549,00 Kč
FSA-LIC-WIN11-1 FortiSandbox Windows Licenses Addon FortiSandbox license of Microsoft Windows 11 by 1. No Universal VM included. [dodávka softwaru]	ks	4	6 294,00 Kč	25 176,00 Kč
FC1-10-FSV00-1035-02-60 FortiSandbox VM00 5 Year Expands FortiSandbox capacity by 1 VM clone count on Local (including Custom) and Cloud. On VM, allows up to 200 VMs. Offered as subscription service for new and existing Sandboxing VMs. No Microsoft license included. [služby a podpora]	ks	4	31 469,00 Kč	125 876,00 Kč
FSA-UPG-OFFICE2021-1 FortiSandbox Office Licenses Expands FSA (Appliance/VM) licenses of Microsoft Office 2021 by 1. [dodávka softwaru]	ks	4	36 352,00 Kč	145 408,00 Kč
Technická podpora (v rozsahu dle smlouvy) - FC-10-FSV00-500-02-60 Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs. [služby a podpora]				354 387,00 Kč
Technická podpora (v rozsahu dle smlouvy) - integrace softwaru s e-mailovou gateway objednatele FortiMail. [služby a podpora]				67 600,00 Kč
Školení (v rozsahu dle smlouvy)				20 000,00 Kč
Celková cena (Kč bez DPH)				949 996,00 Kč

Příloha č. 3

Kontaktní údaje

Objednatel				
Funkce / oblast	Jméno	Pracovní zařazení	Telefon	E-mail
Dodání softwaru				
Převzetí softwaru				
Dodavatel				
Funkce / oblast				
Dodání softwaru				
Předání softwaru				

Technická podpora výrobce

Základní požadavky

Požadavek	Splnění	Poznámky
Vydávání a dostupnost bezpečnostních updatů / hotfixů / upgradů na webu výrobce softwaru.	Ano	
Přístup do znalostní databáze výrobce softwaru.	Ano	
Možnost kontaktování pracovníků výrobce softwaru za účelem konzultace odborných dotazů v režimu 8×5 v pracovní dny.	Ano	

FortiCare Technical Support

*přístup k aktualizacím softwaru, hlášení problémů výrobci / uplatnění technické podpory výrobce
(vyžaduje vytvoření uživatelského účtu a přihlášení)*

<https://www.fortinet.com/support/contact>

Fortinet Community: Support Forum

komunitní podpora (vyžaduje vytvoření uživatelského účtu a přihlášení)

<https://community.fortinet.com/t5/Support-Forum/bd-p/fortinet-discussion>