
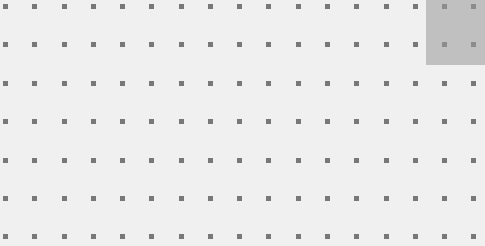
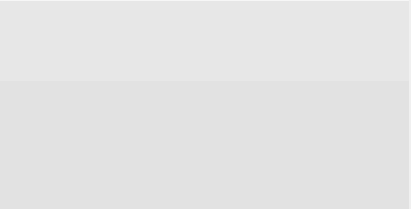




FORTINET®



**Nečekejte, jednejte
aneb jak na nový zákon
o kybernetické bezpečnosti**



Nečekejte, jednejte aneb jak na nový zákon o kybernetické bezpečnosti

Směrnice NIS2 přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již nyní podle aktuálního zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely.

Připravte se na změny

Implementace směrnice NIS2 slibuje výzvy, se kterými se organizace budou muset vypořádat v krátké době. Příprava na soulad se směrnicí NIS2 je nejen zákonným požadavkem, ale také příležitostí, jak posílit odolnost organizace v oblasti kybernetické bezpečnosti.

Čekání na úplnou implementaci směrnice může znamenat, že organizace budou vystaveny potenciálnímu kybernetickým hrozbám a zaostávat v rychle se vyvíjejícím prostředí kybernetické bezpečnosti. Proaktivní vyhodnocení současné bezpečnostní situace a identifikace oblastí, které je třeba zlepšit jsou základními kroky k účinnému řízení kybernetických rizik, splnění přísných požadavků na podávání zpráv a udržení odolné síťové infrastruktury.

Bezpečnost komunikačních sítí



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

Výkonná firewallová platforma FortiGate kombinuje moderní bezpečnostní funkce s hardwarovou akcelerací postavené na technologii ASIC. Díky tomu poskytuje nejen extrémní výkon nutný k segmentaci vnitřní sítě bez zbytečného zatížení procesoru, ale zároveň i extrémně nízkou latenci a minimální závislost na velikosti paketů. Pro další úroveň segmentace mezi prvky ve stejné broadcast doméně je možné doplnit firewall FortiGate o přepínače FortiSwitch, které spolu s firewallem tvoří plně integrované řešení pro segmentaci sítí až na úrovni jednotlivých portů přepínače, a vynutit inspekci provozu v rámci broadcast domény skrze FortiGate FW. Dále možné využít FortiAP a přímo na něm zamezit komunikaci mezi zařízeními připojenými ke stejné bezdrátové síti.

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiAP
Protected LAN Edge deployments with wireless connectivity

ZTNA Agent
Remote access, application access, and risk reduction

FortiGate nabízí funkci IPSec VPN pro bezpečné propojení centrály, poboček a zároveň vzdálený přístup uživatelů k interním systémům. Funkce SSL VPN umožňuje vzdálený přístup uživatelů právě pomocí protokolu SSL. Všechny přístupy jsou řízeny na základě identity uživatele a lze na ně uplatnit libovolný ochranný profil (DLP, AV, IPS, AppCtrl, URL filtering atd.). Dále je možné využít funkci ZTNA, která kombinuje produkty FortiGate FW a FortiClient, díky kterému je možné povýšit IPSec VPN řešení o kontrolu stavu samotné stanice a její autentizaci na základě splnění compliance požadavků a navíc o možnost transparentního sestavení šifrovaného spojení z pracovní stanice k FortiGate FW pro definované cíle bez nutnosti akce uživatele. V případě WiFi sítí je možné využít FortiAP a vynutit, v tunelovém režimu bezdrátové sítě, přenos dat uživatele mezi lokálním FortiAP a centrálním kontrolerem v šifrovaném kanálu CAPWAP protokolu.

FortiManager
Centralized management of your Fortinet security infrastructure

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

Umožňuje vzdálenou správu FortiGate, FortiSwitch, FortiAP, FortiExtender, ... včetně možnosti nastavení administrátorských rolí a oddělení jednotlivých fyzických zařízení nebo virtuálních kontextů v rámci samostatných administrativních domén nástroje FortiManager. Pokud zákazník preferuje centrální správu v cloudu, je k dispozici cloudové management rozhraní FortiCloud.

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiSASE
Enforce dynamic network access control and network segmentation

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

ZTNA Agent
Remote access, application access, and risk reduction

Centrální autentizační server FortiAuthenticator umožňuje plně spravovat prostředí kryptografických klíčů (PKI). V kombinaci s moderními kryptografickými algoritmy použitými pro vzdálený přístup a šifrování pak umožňuje komplexně zabezpečit celou spravovanou síť. Dále je možné využít řešení Fortinet ZTNA, které kombinuje produkty FortiGate FW a FortiClient, díky kterému je možné povýšit IPSec VPN řešení o kontrolu stavu samotné stanice a její autentizaci na základě splnění compliance požadavků a navíc o možnost transparentního sestavení šifrovaného spojení z pracovní stanice k FortiGate FW pro definované cíle bez nutnosti akce uživatele. Pro uživatele pracující z home office lze využít FortiSASE, které běží v cloudu jako služba a umožní poskytnout stejnou úroveň zabezpečení jako on-prem FW/Proxy.

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiToken
One-time password application with push notification

FortiToken Mobile
One-time password application with push notification

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

Všechny platformy uvedené v tomto dokumentu umožňují ověřovat jména a hesla buďto lokálně nebo proti centralizovanému autentizačnímu serveru. Je samozřejmě možné využít stávající autentizační nástroje v síti, nebo využít centrální autentizační server Fortinetu - FortiAuthenticator. V takovém případě získáte plně integrované řešení jednoho výrobce. Zabezpečení přístupu lze dále rozšířit o dvoufaktorovou autentizaci na základě jednorázových hesel generovaných pomocí emailů, SMS, nebo HW a SW tokenů. Platforma FortiPAM toto řešení dále rozšiřuje o správu privilegovaných účtů a to včetně auditu všech událostí. FortiPAM kombinuje funkcionalitu PAM a ZTNA pro zabezpečení bezpečného webového přístupu ověřených privilegovaných uživatelů z prostředí webového prohlížeče, případně nativní aplikace.



Zajišťování dostupnosti regulované služby



Řízení přístupových oprávnění



Aplikační bezpečnost



Kryptografické algoritmy



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiADC
Application-aware intelligence for distribution of application traffic

FortiWeb
Prevent web application attacks against critical web assets

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiDDoS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

Všechna naše zařízení plně podporují režim vysoké dostupnosti, včetně geografické redundance. Zálohování konfiguračních souborů je možné jak v rámci Fortinet centrální správy, tak s využitím obecných platform/platformem třetích stran. Firewall FortiGate díky integrovaným funkcím rozdělování zátěže a secure SD-WAN umožňuje nasazení v prostředí s vysokými nároky na výkonost a dostupnost, jako jsou například datová centra. Pro pokročilé metody rozkládání zátěže (4 - 7 vrstva) je též možné využít dedikovanou platformu FortiADC s vysokou propustností. FortiWeb umožňuje pokročilé rozkládání provozu mezi aplikačními servery v rámci L7 vrstvy. FortiGSLB je cloud-based DNS nástroj pro monitorování dostupnosti služeb zákazníka a přesměrování provozu na záložní/alternativní DNS záznamy definované zákazníkem. FortiDDoS je inline řešení umožňující ochránit organizaci plně automatizovaným rozhodnutím bez nutnosti obsluhy do 1 sekundy před mnoha útoky typu Distributed Denial of Service.

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiSandbox
Secure virtual runtime environment to expose unknown threats

FortiDeceptor
Discover active attackers inside with decoy assets

FortiWeb
Prevent web application attacks against critical web assets

FortiEDR
Automated protection and orchestrated incident response

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

Firewall FortiGate nabízí vícevrstvou ochranu před pokročilými bezpečnostními hrozbami (ATP). Za tímto účelem vhodně kombinuje systém detekce průniku (IPS), antivirové ochrany (AV), detekce typu aplikací (Application Control) a kategorizace přístupu k webovým stránkám (URL filtering). Součástí tohoto systému je i detekce a blokování komunikace s botnet řídicími centry (Botnet C&C). Systém je dále možné rozšířit o FortiSandbox (plnohodnotný customizovatelný sandbox pro analýzu a detekci doposud neidentifikovaných škodlivých kódů bez nutnosti nahrávání dat kamkoliv mimo zákaznicko prostředí. Další možností jak posílit detekci útoku je nasazení technologie honeypotu v podobě FortiDeceptoru. Toto řešení pomáhá detekovat útočníka, kterému se z jakéhokoliv důvodu podařilo proniknout do vnitřní sítě. Web aplikační firewall chrání před hrozbami OWASP TOP 10 s využitím moderních metod jako je využití machine learningu, ochrana API a ochrana před internetovými boty. FortiNDR sleduje síťový provoz a detekuje v něm anomálie, které by mohly představovat hrozbu.

FortiDast
application security testing solution

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiManager
Centralized management of your Fortinet security infrastructure

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

Nástroj FortiDAST představuje automatizovaný nástroj pro penetrační testování formou služby poskytované z cloud prostředí výrobce či jako onprem/proxy řešení. Zahrnuje v sobě testy webových služeb dle specifikace OWASP Top 10. Test může být naplánovaný v pravidelných intervalech nebo aktivován na vyžádání. Identifikovaná rizika jsou reportována, k nalezeným vulnerabilitám je připojeno CVSS skóre. FortiTester slouží primárně jako nástroj pro testování výkonnostních parametrů, ale obsahuje v sobě i modul Breach Attack Simulation, který se hojně využívá pro penetrační testování. Dle specifikace popsané v MITRE ATT&CK umožňuje provádění simulovaného penetračního testování, které využívá aktuální databázi CVE zranitelností, což lze s výhodou využít k ověření kvality např. IPS engine. Dále je k dispozici i modul pro testování typu fuzzing, Web/IoT útoky, testování malware strike pack (včetně zhruba 20 variant ransomware), testování odolnosti proti útokům typu DoS/DDoS a podporována je i možnost práce s vlastním PCAP zdrojem. FortiDevSec je cloudový automatizovaný nástroj pro zabezpečení aplikací, který provádí komplexní skenování pro vyhodnocení zranitelností aplikace. Integruje testování zabezpečení aplikací do prostředí DevOps a začleňuje se do procesu vývoje a nasazování aplikací, aby vyhodnotil a odhalil bezpečnostní nedostatky, které je možné v průběhu životního cyklu vývoje softwaru zmírnit nebo odstranit. FortiManager sleduje instalovanou bázi zařízení a dokáže upozornit na to, když některé zařízení není podporované nebo jeho podpora vypršela. FortiCNP - Cloud Native Protection je řešení, které umožňuje nacházet miskonfigurace cloud prostředí typu AWS, Azure, Google Cloud, skenovat container registry na zranitelnosti nebo datová cloud úložiště na malware/DLP a obecně vyhodnocovat rizika v cloud prostředí.

FortiGate (VPN, ZTNA)
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator (CA)
Identify users wherever they are and enforce strong authentication

FortiManager (CA)
Centralized management of your Fortinet security infrastructure

Všechny produkty využívají a podporují moderní šifrovací algoritmy, konfiguračně je možné zablokovat použití slabých šifer, které by mohly znamenat bezpečnostní riziko. Hlavní součástí kryptografických algoritmů jsou certifikační autority produktů FortiAuthenticator, FortiManager, EMS pro FortiClienta a ZTNA a FortiGate (VPN, ZTNA).

Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv



FortiCamera
HDTV-quality surveillance cameras for physical safety and security



FortiRecorder
High-performance NVR with AI-powered video management software

FortiCamera a její serverová část FortiRecorder tvoří bezpečnostní platformu pro sledování a ochranu jak venkovních, tak vnitřních prostor, umožňuje archivaci natočených záběrů a snadné vyhledávání kritických momentů. Díky odolnosti proti vlivům vnějšího prostředí, nočnímu snímání a především díky management rozhraní shodnému s dalšími produkty společnosti Fortinet, zapadá toto řešení do jednotného konceptu komplexního zabezpečení.

Nástroj FortiPresence dovoluje monitorovat výskyt osob v kontrolovaných oblastech pomocí sledování WiFi signálu jejich mobilních zařízení. Používá se pro monitorování výskytu a triangulaci pozice v sledovaných oblastech

FortiPresence
xxxxxxx



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN



FortiAuthenticator
Identify users wherever they are and enforce strong authentication

Všechny platformy uvedené v tomto dokumentu umožňují ověřovat jména a hesla buďto lokálně nebo proti centralizovanému autentizačnímu serveru. Je samozřejmě možné využít stávající autentizační nástroje v síti, nebo využít centrální autentizační server Fortinetu - FortiAuthenticator. V takovém případě získáte plně integrované řešení jednoho výrobce. Zabezpečení přístupu lze dále rozšířit o dvoufaktorovou autentizaci na základě jednorázových hesel generovaných pomocí emailů, SMS, nebo HW a SW tokenů. Platforma FortiPAM toto řešení dále rozšiřuje o správu privilegovaných účtů a to včetně auditu všech událostí. FortiPAM kombinuje funkcionalitu PAM a ZTNA pro zabezpečení bezpečného webového přístupu ověřených privilegovaných uživatelů z prostředí webového prohlížeče, případně nativní aplikace.



FortiToken
One-time password application with push notification



FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems



FortiTokenMobile
One-time password application with push notification



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN



FortiGate Rugged
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

Firewall FortiGate a jeho varianta určená pro provoz v průmyslovém prostředí (FortiGate Rugged) využívá tentýž operační systém stejně jako všechny další bezpečnostní funkce, avšak liší se HW konstrukcí. FortiGate je určen pro nasazení v klasických datových centrech, tedy na pozici centrálního bodu; FortiGate Rugged pak splňuje požadavky pro nasazení v problematických prostředích (vysoká prašnost, elektromagnetické rušení, atd.). Obě platformy poskytují kompletní ochranu pro průmyslové systémy jak na úrovni firewallu, tak na úrovni detekce konkrétních průmyslových aplikací a detekce a zastavení známých hrozeb útočících na průmyslové protokoly. V místech, kde je potřeba řešit segmentaci přístupové vrstvy lze s výhodou použít FortiSwitch, který se rovněž nabízí v průmyslové podobě.



FortiSwitch
Deliver security, performance, and manageable access to data



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN



FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

Centrální autentizační server FortiAuthenticator umožňuje plně spravovat prostředí kryptografických klíčů (PKI). V kombinaci s moderními kryptografickými algoritmy použitými pro vzdálený přístup a šifrování pak umožňuje komplexně zabezpečit celou spravovanou síť. Dále je možné využít řešení Fortinet ZTNA, které kombinuje produkty FortiGate FW a FortiClient, díky kterému je možné povýšit IPSec VPN řešení o kontrolu stavu samotné stanice a její autentizaci na základě splnění compliance požadavků a navíc o možnost transparentního sestavení šifrovaného spojení z pracovní stanice k FortiGate FW pro definované cíle bez nutnosti akce uživatele.

Pro uživatele pracující z home office lze využít FortiSASE, které běží v cloudu jako služba a umožní poskytnout stejnou úroveň zabezpečení jako on-prem FW/Proxy.



ZTNA Agent
Remote access, application access, and risk reduction



FortiSASE
Enforce dynamic network access control and network segmentation



FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN



FortiGate Rugged
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

Pomocí rozšiřující licence je možné aktivovat ochranu před známými hrozbami zaměřenou výhradně do průmyslové protokoly. Pomocí tohoto nástroje je možné efektivně blokovat pokusy o útoky na zriatelné systémy průmyslového řízení a jejich komponenty. Dále je možné aktivovat modul rozpoznávání průmyslových protokolů na aplikační vrstvě, který lze využít např. v bezpečnostní politice tím způsobem, že rozlišuje jednotlivé příkazy v průmyslových řídicích protokolech s cílem definovat povolené a zakázané příkazy a uplatňovat je na procházející komunikaci.

Fyzická bezpečnost



FortiCamera
HDTV-quality surveillance cameras for physical safety and security




FortiRecorder
High-performance NVR with AI-powered video management software


FortiCamera a její serverová část FortiRecorder tvoří bezpečnostní platformu pro sledování a ochranu jak venkovních, tak vnitřních prostor, umožňuje archivaci natočených záběrů, snadné vyhledávání kritických momentů, detekci obličejů a podezřelých předmětů (například zbraň). Díky odolnosti proti vlivům vnějšího prostředí, nočnímu snímání a především díky management rozhraní shodnému s dalšími produkty společnosti Fortinet, zapadá toto řešení do jednotného konceptu komplexního zabezpečení.

Správa a ověřování identit



 **FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

 **FortiToken**
One-time password application with push notification

 **FortiToken Mobile**
One-time password application with push notification

 **FortiAuthenticator**
Identify users wherever they are and enforce strong authentication

 **FortiPAM**
Control & monitoring of elevated & privileged accounts, processes, and critical systems

Všechny platformy uvedené v tomto dokumentu umožňují ověřovat jména a hesla buďto lokálně nebo proti centralizovanému autentizačnímu serveru. Je samozřejmě možné využít stávající autentizační nástroje v síti, nebo využít centrální autentizační server Fortinetu - FortiAuthenticator. V takovém případě získáte plně integrované řešení jednoho výrobce. Zabezpečení přístupu lze dále rozšířit o dvoufaktorovou autentizaci na základě jednorázových hesel generovaných pomocí emailů, SMS, nebo HW a SW tokenů. Platforma FortiPAM toto řešení dále rozšiřuje o správu privilegovaných účtů a to včetně auditu všech událostí. FortiPAM kombinuje funkcionalitu PAM a ZTNA pro zabezpečení bezpečného webového přístupu ověřených privilegovaných uživatelů z prostředí webového prohlížeče, případně nativní aplikace.

Zaznamenávání událostí




 **FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

 **FortiNAC**
Visibility, access control and automated responses for all networked devices

NGFW funkce detekce zařízení umí rozpoznávat zařízení v síti a kategorizovat je příslušným způsobem; FortiNAC je z pohledu sledování změn v síti ještě pokročilejší, nabízí řadu funkcí včetně automatizace. FortiNAC umožňuje přímou a nepřímou detekci zařízení připojených v síti zákazníka a jejich identifikaci (výrobce, OS, ...) pomocí služby FortiGuard a jejich archivaci pro následné sledování jejich přítomnosti v síti.

 **Fortinet Security Fabric**
The industry's highest-performing integrated cybersecurity mesh platform

Samozřejmostí je synchronizace času napříč produktovým portfliem nebo možnost vyžvořit NTP server např. pomocí FortiGate


 **FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric

 **FortiSIEM**
Integrated security, performance, and availability monitoring


FortiAnalyzer je protokolovací a monitorovací zařízení, které sbírá a vyhodnocuje data generovaná uvnitř sítě, včetně e-mailů. Z jednoho místa je tedy možné monitorovat síťový provoz, ukládat a vyhodnocovat vytvořené záznamy stejně jako vytvářet přehledné bezpečnostní analýzy. FortiSIEM je plnohodnotné SIEM řešení, které dokáže přijímat a zpracovávat události z celé řady různých zařízení různých výrobců, využívá strojového učení pro detekci neobvyklého chování uživatelů (UEBA), obsahuje konfigurační databázi (CMDB) s automatickým naplněním logujících zařízení a umožňuje kombinovat pohled SOC a NOC týmu.


Vyhodnocování kybernetických bezpečnostních událostí




 **FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric


 **FortiSIEM**
Integrated security, performance, and availability monitoring


 **FortiRecon**
Digital Risk Protection (DRP) for early, actionable warning and fast response


 **SOC-as-a-Service**
Continuous awareness and control of events, alerts, and threats

 **FortiEDR**
Automated protection and orchestrated incident response

 **FortiSandbox**
Secure virtual runtime environment to expose unknown threats

 **FortiSOAR**
Automated security operations, analytics, and response

 **FortiINDR**
Accelerate mitigation of evolving threats and threat investigation

 **FortiDeceptor**
Discover active attackers inside with decoy assets

 **FortiGuard Threat Intelligence**

FortiAnalyzer je protokolovací a monitorovací zařízení, které sbírá a vyhodnocuje data generovaná uvnitř sítě, včetně e-mailů.

Z jednoho místa je tedy možné monitorovat síťový provoz, ukládat a vyhodnocovat vytvořené záznamy stejně jako vytvářet přehledné bezpečnostní analýzy.

FortiSIEM je plnohodnotné SIEM řešení, které dokáže přijímat a zpracovávat události z celé řady různých zařízení různých výrobců.

FortiRecon je nástroj tzv. včasného varování, který slouží k monitoringu informací na internetu a darknetu, vztahujících se na chráněný objekt/síť/uživatele... Dovoluje také procházet sociální sítě, registrované domény, repozitáře různých app store a další zdroje a vyhledávat možné souvislosti s chráněným subjektem. Pokud se někde objeví např. ukradená citlivá data, podvržené domény nebo aplikace, uživatel je okamžitě upozorněn a služba dovoluje rovněž spustit proces zablokování daného zdroje.

FortiSOCaaS je služba nabízející zákazníkovi funkcionalitu Security Operation Center poskytovanou jako službu od společnosti Fortinet. Pro vytvoření SOCu zákazníkem/partnerem lze s výhodou využít produktů FortiEDR (Endpoint Detect Response), FortiINDR (Network Detect Response), FortiSandbox, FortiSOAR (Security Orchestration, Automation and Response) a dalších. Další možností jak posílit detekci útoku je nasazení technologie honeypotu v podobě FortiDeceptoru. Toto řešení pomáhá detekovat útočníka, kterému se z jakéhokoliv důvodu podařilo proniknout do vnitřní sítě. Všechny naše produkty využívají službu FortiGuard jako zdroj informací a signatur definujících aktuální hrozby. Služba FortiGuard využívá nástroje AI (umělé inteligence) a také samostatný team vývojářů pro testování všech zveřejňovaných signatur s cílem zamezit chybnému vyhodnocování bezpečnostních událostí.

 **FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

 **FortiCNP**
Manage risk and compliance through multi-cloud infrastructures

V rámci FortiGate je dostupná funkce Security Rating, která vyhodnocuje konfiguraci a bezpečnostní rizika a navrhuje vylepšení. FortiCNP - Cloud Native Protection je řešení, které umožňuje nacházet misconfigurace cloud prostředí typu AWS, Azure, Google Cloud, skenovat container registry na zranitelnosti nebo datová cloud úložiště na malware/DLP a obecně vyhodnocovat rizika v cloud prostředí.

Vyhodnocování
kybernetických
bezpečnostních
událostí



SOC-as-a-Service

Continuous awareness and
control of events, alerts,
and threats



Data Sheet

FortiGuard SOC as a Service



FORTINET Data Sheet

FortiGuard SOC as a Service



Top Benefits

- **Reduce SOC Triage Effort** - Automate and reduce manual tasks, allowing you to focus on high-priority alerts.
- **24x7 Monitoring** - FortiGuard SOC provides 24x7 monitoring and incident response support to ensure your network is always protected.
- **Reduce Cyber Risk** - Proactive threat hunting, vulnerability scanning, and threat intelligence help you identify and mitigate risks before they become incidents.
- **Streamline Incident Response** - Automated workflows and playbooks speed up incident response and reduce the time to resolution.
- **Scale Your Security** - FortiGuard SOC scales to meet your needs, providing a cost-effective solution for businesses of all sizes.

Fortinet Managed SOCaaS

Take advantage of Fortinet's Security Operations Center as a Service (SOCaaS). It simplifies SOC management and allows you to focus on your core business while Fortinet handles your security operations and incident response.

The Benefits

Optimized 24x7 Monitoring

- Offload monitoring your network to Fortinet's SOC 24x7
- 24x7 threat hunting with our advanced AI/ML engine

Streamline Incident Response with Expert Insights

- Gain expert insights into any alerts and investigate security incidents
- Reduce incident resolution time with response playbooks and alerts

Simplify Operations

- Reduce a heavy burden with predictable security operations
- Reduce operational complexity

FORTINET Data Sheet

FortiGuard SOC as a Service



Global Response Time

- Asia Pacific: 15 minutes
- Europe: 15 minutes
- North America: 15 minutes
- Latin America: 30 minutes
- Africa & Middle East: 30 minutes

Critical Escalation Times

- P1 Priority: 15 minutes
- P2 Priority: 45 minutes
- P3 Priority: 90 minutes
- P4 Priority: 4 hours

Let Fortinet monitor and investigate Fortinet alerts and notifications 24x7 only notifying you about concerning or important and resolve incidents.

Fortinet security experts utilize teams in as little as 15 minutes and provide insights into what happened, why it happened, and what steps to take to resolve the incident.

SOCaaS includes a dedicated person with 24x7 monitoring, incident response, and reporting, and security knowledge with Fortinet security experts who allow users to take the security, report up the chain, replace their security personnel, and reduce alert noise.

FORTINET Data Sheet

FortiGuard SOC as a Service

Benefits

Time Savings	Proactive Action	Maximized Investment
<ul style="list-style-type: none"> • Supplement Fortinet logs with alert monitoring and logs with Fortinet security experts • Reduce on-premise hardware and software costs over a 3-year period • Complete 24x7 global coverage with low incident response 	<ul style="list-style-type: none"> • Reduce operational issues in a 24x7 environment • Reduce security operations and threat response • Why it happened • Impact • Remediation • Fortinet support for city operations 	<ul style="list-style-type: none"> • Highlight alerts of high severity and provide additional context and intelligence • Enhance security operations and incident response • Enhance security, reducing time, and reducing response time

Ordering Information

Note that SOCaaS is a cloud solution for any Fortinet device or Fortinet logs to be monitored directly to SOCaaS, but also typically for devices from the Fortinet FortiGuard ecosystem, on-premise or in the cloud.

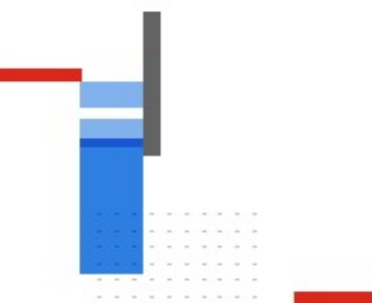
Contact your Fortinet account manager for more information on SOCaaS or contact us at sales@fortinet.com.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to doing business with responsibility, with a goal for human rights and environmental protection, making products a digital world that is safe, secure, and reliable for Fortinet that you will use as Fortinet products are critical to people, or support in any way, facilitate or abuse of human rights, including those involving digital economy, surveillance, censorship, or excessive use of Internet users of Fortinet products are required to comply with the Fortinet Code of Conduct and support any applicable standards of the Code via the procedures outlined in the Fortinet Environmental Policy.

FORTINET Data Sheet

FortiGuard SOC as a Service



Fortinet

© Fortinet Inc. All Rights Reserved.





Fortinet Security Fabric The industry's highest-performing integrated cybersecurity mesh platform

➔ Product Matrix
 ✎ Click on icons in this document for additional information

Fortinet Brochure
 Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
 Fortinet is committed to training over 1 million people by 2025

Free Assessment
 Perform an assessment in your network to validate your existing controls

FortiOS
 The Heart of the Fortinet Security Fabric

Secure Networking

- FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiGate SD-WAN**
Application-centric, scalable, and Secure SD-WAN with NGFW
- FortiExtender**
Extend scalable and resilient LTE and LAN connectivity
- FortiAP**
Protected LAN Edge deployments with wireless connectivity
- FortiSwitch**
Deliver security, performance, and manageable access to data
- FortiNAC**
Visibility, access control and automated responses for all networked devices
- FortiProxy**
Enforce internet, compliance and granular application control
- Fortisolator**
Maintain an "air-gap" between browser and web content

Cloud Security

- FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiDDoS**
Machine-learning quickly inspects traffic at layers 3, 4, and 7
- FortiCNP**
Manage risk and compliance through multi-cloud infrastructures
- FortiDevSec**
Continuous application security testing in CI/CD pipelines
- FortiWeb**
Prevent web application attacks against critical web assets
- FortiADC**
Application-aware intelligence for distribution of application traffic
- FortiGSLB Cloud**
Ensure business continuity during Unexpected network downtime
- FortiMail**
Secure mail gateway to protect against SPAM and virus attacks
- FortiCASB**
Prevent misconfigurations of SaaS applications and meet compliance
- FortiCNF**
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

- FortiSASE**
Enforce dynamic network access control and network segmentation
- ZTNA Agent**
Remote access, application access, and risk reduction
- FortiAuthenticator**
Identify users wherever they are and enforce strong authentication
- FortiToken**
One-time password application with push notification
- FortiClient Fabric Agent**
IPSec and SSL VPN tunnel, endpoint telemetry and more
- FortiGuest**
Simplified guest access, BYOD, and policy management
- FortiPAM**
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence



Fabric Management Center: NOC

- FortiManager**
Centralized management of your Fortinet security infrastructure
- FortiGate Cloud**
SaaS w/ zero touch deployment, configuration, and management
- FortiMonitor**
Analysis tool to provide NOC and SOC monitoring capabilities
- FortiAIops**
Network inspection to rapidly analyze, enable, and correlate
- FortiExtender Cloud**
Deploy, manage and customize LTE internet access
- FNDN**
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem
 The industry's most extensive ecosystem of integrated solutions

- Fabric Connectors**
Fortinet-developed
- DevOp Tools & Script**
Fortinet & community-driven
- Fabric API Integration**
Partner-led
- Extended Ecosystem**
Threat sharing w/ tech vendors

Fabric Management Center: SOC

- FortiDeceptor**
Discover active attackers inside with decoy assets
- FortiNDR**
Accelerate mitigation of evolving threats and threat investigation
- FortiEDR**
Automated protection and orchestrated incident response
- FortiRecon**
Digital Risk Protection (DRP) for early, actionable warning and fast response
- FortiSandbox / FortiAI**
Secure virtual runtime environment to expose unknown threats
- FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric
- FortiSIEM**
Integrated security, performance, and availability monitoring
- FortiSOAR**
Automated security operations, analytics, and response
- FortiTester**
Network performance testing and breach attack simulation (BAS)
- SOC-as-a-Service**
Continuous awareness and control of events, alerts, and threats
- Incident Response Service**
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

- FortiCare Essentials***
15% of hardware
- FortiCare Premium***
20% of hardware
- FortiCare Elite****
25% of hardware
- FortiConverter**
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs
 ** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

- FortiFone**
Robust IP Phones w/ HD Audio with centralized management
- FortiVoice**
Integrated voice, chat, conferencing management, and fax with centralized
- FortiCamera**
HDTV-quality surveillance cameras for physical safety and security
- FortiRecorder**
High-performance NVR with AI-powered video management software



A Technology and a Learning Partner

Fortinet NSE Certification Program (FREE)

An 8-level training and assessment program designed for customers, partners, and employees

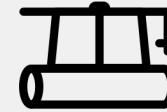
Free Public Network Security Expert Training*

Fortinet has opened up our entire self-paced catalogue of advanced Network Security Expert training courses.

Step	Level Objective
 NSE 1	Security Associate
 NSE 2	Security Associate
 NSE 3	Security Associate
 NSE 4	Professional
 NSE 5	Analyst
 NSE 6	Specialist
 NSE 7	Architect
 NSE 8	Expert



770,000+
CERTIFICATIONS



400+
ACADEMIES

20+

Education Outreach
partners



90+
COUNTRIES &
TERRITORIES

* Instructor-led courses, hands-on labs, and certifications are not included.

Figures as of Dec. 31, 2021





Fortinet Security Fabric The industry's highest-performing integrated cybersecurity mesh platform

➔ Product Matrix
 ✎ Click on icons in this document for additional information

Fortinet Brochure
 Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
 Fortinet is committed to training over 1 million people by 2025

Free Assessment
 Perform an assessment in your network to validate your existing controls

FortiOS
 The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
 NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
 Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
 Extend scalable and resilient LTE and LAN connectivity

FortiAP
 Protected LAN Edge deployments with wireless connectivity

FortiSwitch
 Deliver security, performance, and manageable access to data

FortiNAC
 Visibility, access control and automated responses for all networked devices

FortiProxy
 Enforce internet, compliance and granular application control

FortiSolator
 Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
 NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
 Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
 Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
 Continuous application security testing in CI/CD pipelines

FortiWeb
 Prevent web application attacks against critical web assets

FortiADC
 Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
 Ensure business continuity during Unexpected network downtime

FortiMail
 Secure mail gateway to protect against SPAM and virus attacks

FortiCASB
 Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
 Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
 Enforce dynamic network access control and network segmentation

ZTNA Agent
 Remote access, application access, and risk reduction

FortiAuthenticator
 Identify users wherever they are and enforce strong authentication

FortiToken
 One-time password application with push notification

FortiClient Fabric Agent
 IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
 Simplified guest access, BYOD, and policy management

FortiPAM
 Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence



Fabric Management Center: NOC

FortiManager
 Centralized management of your Fortinet security infrastructure

FortiGate Cloud
 SaaS w/ zero touch deployment, configuration, and management

FortiMonitor
 Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIops
 Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
 Deploy, manage and customize LTE internet access

FNDN
 Exclusive developer community for access to advanced tools & scripts

Open Ecosystem
 The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
 Fortinet-developed

DevOp Tools & Script
 Fortinet & community-driven

Fabric API Integration
 Partner-led

Extended Ecosystem
 Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
 Discover active attackers inside with decoy assets

FortiNDR
 Accelerate mitigation of evolving threats and threat investigation

FortiEDR
 Automated protection and orchestrated incident response

FortiRecon
 Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
 Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
 Correlation, reporting, and log management in Security Fabric

FortiSIEM
 Integrated security, performance, and availability monitoring

FortiSOAR
 Automated security operations, analytics, and response

FortiTester
 Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
 Continuous awareness and control of events, alerts, and threats

Incident Response Service
 Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
 15% of hardware

FortiCare Premium*
 20% of hardware

FortiCare Elite**
 25% of hardware

FortiConverter
 25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs
 ** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
 Robust IP Phones w/ HD Audio with centralized management

FortiVoice
 Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
 HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
 High-performance NVR with AI-powered video management software



- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- System
- Security Fabric**
 - Physical Topology
 - Logical Topology
 - Security Rating**
 - Automation
 - Fabric Connectors
 - External Connectors
 - Asset Identity Center
 - Log & Report

Security Posture Identify configuration weaknesses and best practice violations in your deployment.

Security Control Results

B

255.44

Report Details

Score: 255.44
 Last Ran: 13 seconds ago
 Endpoints: 19

Trends

High: 255.44
 Low: 255.44
 Change: 0.00%

Grades

C Fabric Security Hardening	B Firmware & Subscriptions
A Audit Logging & Monitoring	F Endpoint Management
F Threat & Vulnerability Management	F FortiGuard Outbreak Detection

Search

FSBP PCI Export All

Security Control	Device	Score	Result	Compliance
Endpoint Registration <small>Interfaces which are classified as "LAN" and are used by a policy should have Security Fabric Connection enabled.</small>	EZ	-30	Failed	FSBP EM01.1
FortiGuard IoT Vulnerability <small>IoT devices shouldn't have any security vulnerabilities.</small>		-30	Unmet Dependencies	FSBP EM03.1
Valid HTTPS Certificate - Administrative GUI <small>The administrative GUI should be using a valid and secure certificate.</small>		-30	Failed	FSBP SH03.1
Admin Password Policy <small>A password policy should be set up for system administrators.</small>	EZ	-10	Failed	FSBP SH05.1
Admin Password Security <small>The password policy should enforce secure passwords.</small>		-10	Unmet Dependencies	FSBP SH05.2

Exempt 3

Admin Password Policy

A password policy should be set up for system administrators.

Category

Fabric Security Hardening (SH)

Recommendations

Backup configuration before applying

-10 EZ

Enable a simple password policy for system administrators. By default, the password policy will enforce a minimum password length of 8 characters.

Visit the following page(s) to remediate:

[System > Settings](#)

Apply

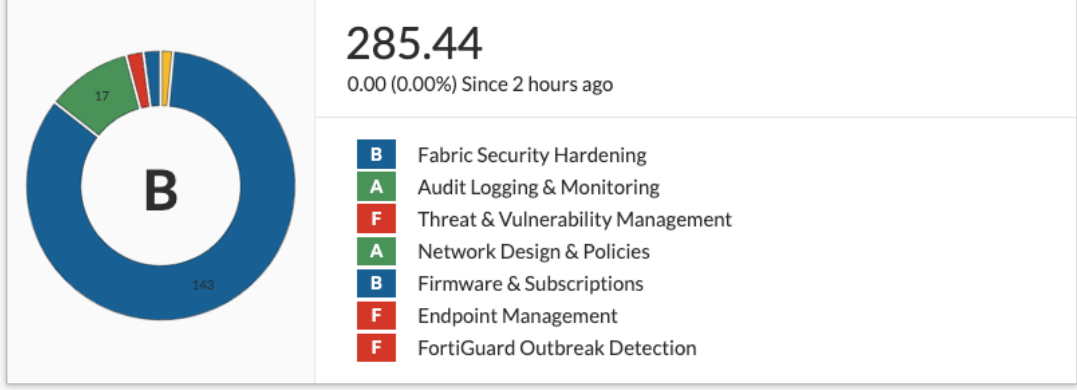
100% 55

Total Score: -10



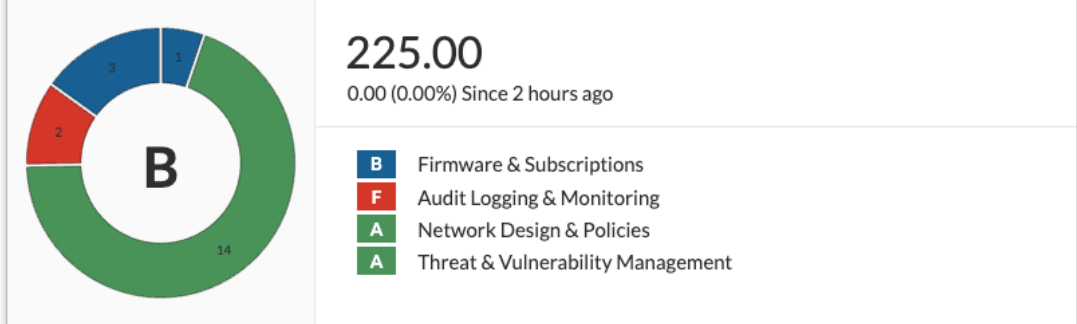
Security Posture

Identify configuration weaknesses and best practice violations in your deployment.



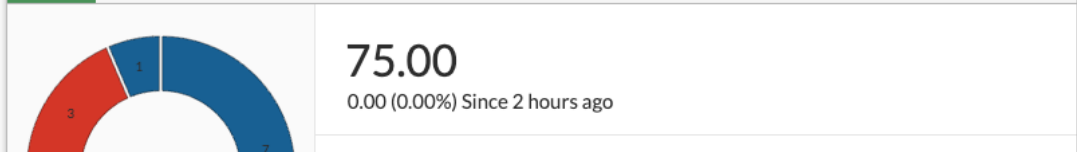
Fabric Coverage

Identify in your overall network, where Security Fabric can enhance visibility and control.



Optimization

Optimize your fabric deployment.



Report Details

Last Ran

2 hours, 27 minutes and 32 seconds ago

[Run Now](#)

Endpoint Snapshot

Total Endpoints

19

Total Endpoints Change

Device Types

- 8 Apple
- 4 Generic
- 3 Windows
- 2 FortiSwitch
- 1 Tablet
- 1 FortiAP



Online Guides

- [Relevant Documentation](#)
- [Video Tutorials](#)

Hot Questions at FortiAnswers

[Join the Discussion](#)



Fortinet Security Fabric The industry's highest-performing integrated cybersecurity mesh platform

➔ Product Matrix
 ✎ Click on icons in this document for additional information

Fortinet Brochure
 Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
 Fortinet is committed to training over 1 million people by 2025

Free Assessment
 Perform an assessment in your network to validate your existing controls

FortiOS
 The Heart of the Fortinet Security Fabric

Secure Networking

- FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiGate SD-WAN**
Application-centric, scalable, and Secure SD-WAN with NGFW
- FortiExtender**
Extend scalable and resilient LTE and LAN connectivity
- FortiAP**
Protected LAN Edge deployments with wireless connectivity
- FortiSwitch**
Deliver security, performance, and manageable access to data
- FortiNAC**
Visibility, access control and automated responses for all networked devices
- FortiProxy**
Enforce internet, compliance and granular application control
- Fortisolator**
Maintain an "air-gap" between browser and web content

Cloud Security

- FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiDDOS**
Machine-learning quickly inspects traffic at layers 3, 4, and 7
- FortiCNP**
Manage risk and compliance through multi-cloud infrastructures
- FortiDevSec**
Continuous application security testing in CI/CD pipelines
- FortiWeb**
Prevent web application attacks against critical web assets
- FortiADC**
Application-aware intelligence for distribution of application traffic
- FortiGSLB Cloud**
Ensure business continuity during Unexpected network downtime
- FortiMail**
Secure mail gateway to protect against SPAM and virus attacks
- FortiCASB**
Prevent misconfigurations of SaaS applications and meet compliance
- FortiCNF**
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

- FortiSASE**
Enforce dynamic network access control and network segmentation
- ZTNA Agent**
Remote access, application access, and risk reduction
- FortiAuthenticator**
Identify users wherever they are and enforce strong authentication
- FortiToken**
One-time password application with push notification
- FortiClient Fabric Agent**
IPSec and SSL VPN tunnel, endpoint telemetry and more
- FortiGuest**
Simplified guest access, BYOD, and policy management
- FortiPAM**
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence



Fabric Management Center: NOC

- FortiManager**
Centralized management of your Fortinet security infrastructure
- FortiGate Cloud**
SaaS w/ zero touch deployment, configuration, and management
- FortiMonitor**
Analysis tool to provide NOC and SOC monitoring capabilities
- FortiAIops**
Network inspection to rapidly analyze, enable, and correlate
- FortiExtender Cloud**
Deploy, manage and customize LTE internet access
- FNDN**
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem
 The industry's most extensive ecosystem of integrated solutions

- Fabric Connectors**
Fortinet-developed
- DevOp Tools & Script**
Fortinet & community-driven
- Fabric API Integration**
Partner-led
- Extended Ecosystem**
Threat sharing w/ tech vendors

Fabric Management Center: SOC

- FortiDeceptor**
Discover active attackers inside with decoy assets
- FortiNDR**
Accelerate mitigation of evolving threats and threat investigation
- FortiEDR**
Automated protection and orchestrated incident response
- FortiRecon**
Digital Risk Protection (DRP) for early, actionable warning and fast response
- FortiSandbox / FortiAI**
Secure virtual runtime environment to expose unknown threats
- FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric
- FortiSIEM**
Integrated security, performance, and availability monitoring
- FortiSOAR**
Automated security operations, analytics, and response
- FortiTester**
Network performance testing and breach attack simulation (BAS)
- SOC-as-a-Service**
Continuous awareness and control of events, alerts, and threats
- Incident Response Service**
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

- FortiCare Essentials***
15% of hardware
 - FortiCare Premium***
20% of hardware
 - FortiCare Elite****
25% of hardware
 - FortiConverter**
25% of hardware
- * FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs
 ** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

- FortiFone**
Robust IP Phones w/ HD Audio with centralized management
- FortiVoice**
Integrated voice, chat, conferencing management, and fax with centralized
- FortiCamera**
HDTV-quality surveillance cameras for physical safety and security
- FortiRecorder**
High-performance NVR with AI-powered video management software





Username:

Password:

Login

WARNING

This information system is the property of Fortinet.
Unauthorized or improper use of this system may result in administrative disciplinary action,
and/or civil charges/criminal penalties.
By continuing to use the system you indicate your awareness of and consent to these terms
and conditions of use. STOP IMMEDIATELY if you do not agree to the conditions stated in
this warning.



FortiToken RB

058532




Login Request

User: rbay

Time: 15:12:03

03 September 2023

Client Application:  fortine

Deny

Approve





Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

➔ Product Matrix
 ✎ Click on icons in this document for additional information

Fortinet Brochure
 Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
 Fortinet is committed to training over 1 million people by 2025

Free Assessment
 Perform an assessment in your network to validate your existing controls

FortiOS
 The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
 NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
 Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
 Extend scalable and resilient LTE and LAN connectivity

FortiAP
 Protected LAN Edge deployments with wireless connectivity

FortiSwitch
 Deliver security, performance, and manageable access to data

FortiNAC
 Visibility, access control and automated responses for all networked devices

FortiProxy
 Enforce internet, compliance and granular application control

FortiSolator
 Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
 NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
 Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
 Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
 Continuous application security testing in CI/CD pipelines

FortiWeb
 Prevent web application attacks against critical web assets

FortiADC
 Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
 Ensure business continuity during Unexpected network downtime

FortiMail
 Secure mail gateway to protect against SPAM and virus attacks

FortiCASB
 Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
 Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
 Enforce dynamic network access control and network segmentation

ZTNA Agent
 Remote access, application access, and risk reduction

FortiAuthenticator
 Identify users wherever they are and enforce strong authentication

FortiToken
 One-time password application with push notification

FortiClient Fabric Agent
 IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
 Simplified guest access, BYOD, and policy management

FortiPAM
 Control & monitoring of elevated & privileged accounts, processes, and critical systems

Fabric Management Center: NOC

FortiManager
 Centralized management of your Fortinet security infrastructure

FortiGate Cloud
 SaaS w/ zero touch deployment, configuration, and management

FortiMonitor
 Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIops
 Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
 Deploy, manage and customize LTE internet access

FNDN
 Exclusive developer community for access to advanced tools & scripts

Fabric Management Center: SOC

FortiDeceptor
 Discover active attackers inside with decoy assets

FortiNDR
 Accelerate mitigation of evolving threats and threat investigation

FortiEDR
 Automated protection and orchestrated incident response

FortiRecon
 Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
 Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
 Correlation, reporting, and log management in Security Fabric

FortiSIEM
 Integrated security, performance, and availability monitoring

FortiSOAR
 Automated security operations, analytics, and response

FortiTester
 Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
 Continuous awareness and control of events, alerts, and threats

Incident Response Service
 Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
 15% of hardware

FortiCare Premium*
 20% of hardware

FortiCare Elite**
 25% of hardware

FortiConverter
 25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs
 ** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

FortiGuard Threat Intelligence

Powered by FortiGuard Labs



Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
 Fortinet-developed

DevOp Tools & Script
 Fortinet & community-driven

Fabric API Integration
 Partner-led

Extended Ecosystem
 Threat sharing w/ tech vendors

Communication and Surveillance

FortiFone
 Robust IP Phones w/ HD Audio with centralized management

FortiVoice
 Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
 HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
 High-performance NVR with AI-powered video management software



APPLICATIONS

Showing 1-10/139

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
<input type="checkbox"/> Google Chrome Signed Google		Critical	2022-11-18 15:12:38	2023-04-17 16:51:55	
<input type="checkbox"/> Microsoft Office Unsigned Microsoft Corporation		Critical	2022-07-20 12:00:15	2023-05-16 10:37:54	
<input type="checkbox"/> Microsoft Edge Signed Microsoft Corporation		Critical	2022-07-18 19:43:02	2023-06-14 02:09:08	
<input type="checkbox"/> <input checked="" type="checkbox"/> Apple ID Signed Apple		Unknown	Critical	2023-04-16 12:43:07	2023-04-16 12:43:07
<input checked="" type="checkbox"/> Firefox Signed Mozilla Corporation		Critical	2022-08-03 22:39:59	2023-06-13 22:42:46	
<input type="checkbox"/> 107.0.1		Critical	2022-11-30 14:55:55	2022-12-09 08:55:52	
<input type="checkbox"/> 112.0.1		Critical	2023-04-20 20:03:13	2023-06-13 22:42:46	
<input type="checkbox"/> 108.0		Critical	2023-01-04 14:55:33	2023-01-23 06:55:47	
<input type="checkbox"/> 107.0		Critical	2022-11-19 19:54:39	2022-11-30 07:56:02	
<input type="checkbox"/> 54.0		Critical	2022-08-03 22:39:59	2022-11-19 19:46:44	
<input type="checkbox"/> <input checked="" type="checkbox"/> Outlook Signed Microsoft Corporation		Unknown	High	2023-04-15 18:40:48	2023-04-17 17:07:46
<input type="checkbox"/> <input checked="" type="checkbox"/> FortiClient Signed Fortinet Inc.		Unknown	High	2022-07-19 08:08:14	2023-01-19 14:53:49
<input type="checkbox"/> <input checked="" type="checkbox"/> Microsoft OneDrive Signed Microsoft Corporation		High	2022-07-19 08:06:02	2023-06-14 02:20:52	
<input type="checkbox"/> <input checked="" type="checkbox"/> Microsoft Excel Signed Microsoft Corporation		Unknown	High	2023-04-15 18:40:40	2023-04-17 17:15:41
<input type="checkbox"/> <input checked="" type="checkbox"/> Microsoft Teams Signed Microsoft Corporation		Medium	2023-04-15 22:42:31	2023-06-14 02:26:57	

VERSION DETAILS

Firefox, v. 107.0

Policies

Servers Policy FORTINET	Deny
MIG_Communication Control Policy	Allow
PK_APPCTRL	Deny
PK_POC	Deny
ROBIN_Communication Control Policy	Deny
Isolation Policy FORTINET	Deny

Vulnerabilities

Total 94 CVEs

- [CVE-2023-34417](#) - Critical (CVSS 3.0: 9.8, CVSS 2.0: null)
- [CVE-2023-34416](#) - Critical (CVSS 3.0: 9.8, CVSS 2.0: null)
- [CVE-2023-32216](#) - Critical (CVSS 3.0: 9.8, CVSS 2.0: null)
- [CVE-2023-29542](#) - Critical (CVSS 3.0: 9.8, CVSS 2.0: null)
- [CVE-2023-25736](#) - Critical (CVSS 3.0: 9.8, CVSS 2.0: null)
- [CVE-2023-37212](#) - High (CVSS 3.0: 8.8, CVSS 2.0: null)
- [CVE-2023-37211](#) - High (CVSS 3.0: 8.8, CVSS 2.0: null)

ADVANCED DATA

APPLICATION INFO

Application Description:	Firefox
First Connection Time:	19-Nov-2022
Last Connection Time:	30-Nov-2022
Process Names:	<ul style="list-style-type: none">\\Device\\HarddiskVolume3\\Users\\test1\\AppData\\Local\\Temp\\7zS4...\\Device\\HarddiskVolume3\\Program Files\\Mozilla Firefox\\firefox.e... And 2 more...

APPLICATION USAGE

No Collectors

DESCRIPTIONS:

IP	CONNECTION TIME
93.184.220.29	30-Nov-2022
34.120.208.123	30-Nov-2022
2.16.2.73	30-Nov-2022

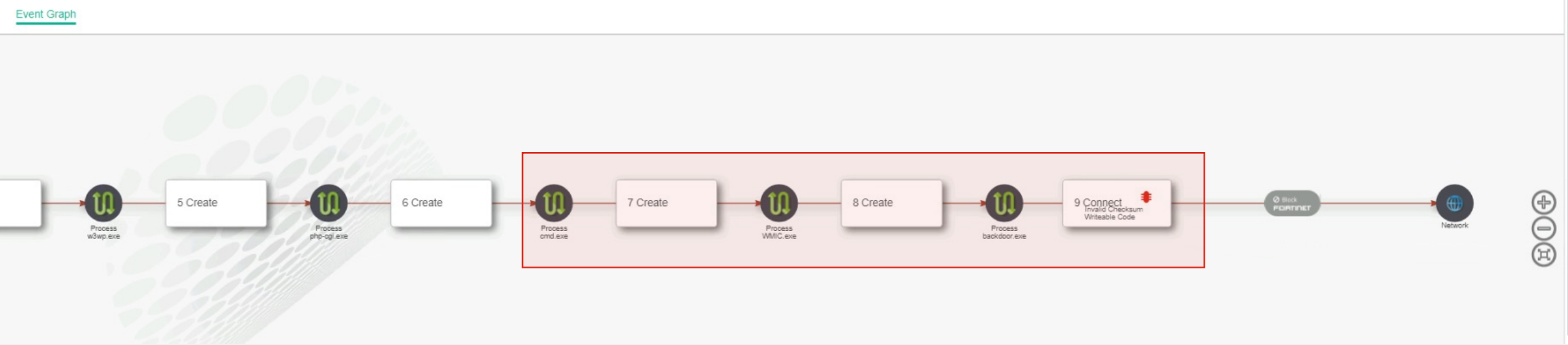
LOCATION
United Kingdom
United States
Czechia

[More...](#)

Event 10416 backdoor.exe | Event 10456 backdoor.exe

Add Exception
Retrieve
Remediate
Isolate
Connect to Device
Export
Raw Data Items: All
Selected 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
SRV-WS-IIS-A1	Windows Server 2019 ...	backdoor.exe	Malicious	Network Access	22-Aug-2023, 05:46:23	22-Aug-2023, 05:46:23	
RAW ID: 1298854625	Process Type: 64 bit	Certificate: Unsigned	Process Path: C:\inetpub\wwwroot\uploads\backdoor.exe	User: None	Count: 1		





Clear All



Event 10416 backdoor.exe

Event 10456 backdoor.exe

Add Exception Retrieve Remediate Isolate Connect to Device Export

Raw Data Items: All Selected 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
SRV-WS-IIS-A1	Windows Server 2019 ...	backdoor.exe	Malicious	Network Access	22-Aug-2023, 05:46:23	22-Aug-2023, 05:46:23	
RAW ID: 1298854625		Process Type: 64 bit	Certificate: Unsigned	Process Path: C:\inetpub\wwwroot\uploads\backdoor.exe	User: None	Count: 1	
<p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p> <p>PARENT PROCESS CREATION</p>							

NETWORK ACCESS ATTEMPT

Process ID: 1280
 Source Process: ...ice\HarddiskVolume2\inetpub\wwwroot\uploads\backdoor.exe
 Target: NET ACCESS

Company:
 Description:
 Version:

Product:
 Comments:
 Command Line:

Process Hash (SHA-1): 895F3697804218CC4845BD552527D2ED38177955
 Process Owner: This O...

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
• Main -\Device\HarddiskVolume2\inetpub\wwwroot\uploads\backdoor.exe	No	Unsigned				895F3697804218CC4845BD552527D2ED38177955
\Device\HarddiskVolume2\Windows\System32\wininet.dll	No	Signed	1	0x7ff89dfe0000	0x7ff89e4c1000	53BC6FAAA0BCC1E1E1F4FE59229F38E023D7FC6
• \Device\HarddiskVolume2\inetpub\wwwroot\uploads\backdoor.exe	Yes	Unsigned	4	0x140000000	0x140005000	895F3697804218CC4845BD552527D2ED38177955
\Device\HarddiskVolume2\inetpub\wwwroot\uploads\backdoor.exe	Yes	Unsigned	1	0x140000000	0x140005000	895F3697804218CC4845BD552527D2ED38177955
\Device\HarddiskVolume2\inetpub\wwwroot\uploads\backdoor.exe	Yes	Unsigned	1	0x140000000	0x140005000	895F3697804218CC4845BD552527D2ED38177955
\Device\HarddiskVolume2\Windows\System32\kernel32.dll	No	Signed	1	0x7ff8b9600000	0x7ff8b96b3000	68A1D9FE214BA35D247D87DCDE61701EE2D38005

895F3697804218CC4845BD552527D2ED38177955

VirusTotal

Threat Hunting

Add to Blocklist





Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

➔ Product Matrix

👆 Click on icons in this document for additional information

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiSolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail gateway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
Simplified guest access, BYOD, and policy management

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
SaaS w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIops
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiRecon
Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

FortiGuard Threat Intelligence

Powered by FortiGuard Labs



Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

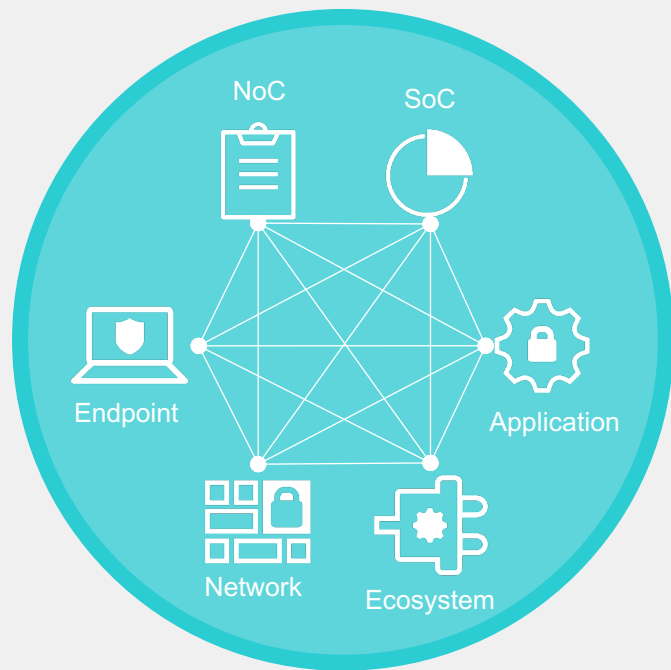
FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software



75% of large organizations are actively pursuing a vendor consolidation strategy

Consolidate Point Products & Vendors into a Cybersecurity Platform



Primary Reasons Organizations are Pursuing Security Vendor Consolidation:

55%

Increase efficacy by integrating multiple components

55%

Increase effectiveness by allowing broader reach and visibility

43%

Easier management by reducing the number of separate tools

35%

Cost/budgeting/to save money

Gartner

Gartner, Cybersecurity Market Insight: Convey Business Outcomes When Marketing Security Solutions Published 11 January 2023

Gartner, Infographic: Top Trends in Cybersecurity 2022 — Vendor Consolidation Published 19 August 2022



FORTINET®