Security solutions

2026

Member of UNITED GROUP

Предизвикателства за бизнеса

99% of пробивите са поради грешки и пропуски в конфигурациите

56% от бизнес клиентите изпитват затруднения да назначат специалисти по киберсигурност

Предизвикателства

Достъпност на услугите
Влияе на бизнеса и конкурентно способността

Рискове свързани със сигурността
Поради постоянно увеличение на кибер атаките

Разходи
Поради мрежова комплексност и липса на квалифициран персонал

Над какво да се замислим

Инвестирайте в предотвратяване на заплахи:

- Използвайте усъвършенствани технологии за сигурност, като системи за предотвратяване на прониквания (IPS), инструменти против рансъмуер.

Укрепете защитата на крайните точки и мрежата:

- Внедрете надеждни защитни стени, защита на имейли и платформи за защита на крайните точки.

Повишете осведомеността:

- Провеждайте редовни обучения и симулирани упражнения за фишинг, за да помогнете на служителите да разпознават и докладват подозрителна активност.

Осигурете готовност за архивиране и възстановяване:

- Поддържайте актуални, сегментирани резервни копия и тествайте редовно процесите на възстановяване.

Приемете принципите на нулево доверие:

- Непрекъснато проверявайте разрешенията за достъп и сегментирайте мрежите.

NIS2

2026

Member of UNITED GROUP

Директива за киберсигурност на ЕС – NIS2

Какво е NIS2

Ключова законодателна инициатива на ЕС с цел подобряване на информационната сигурност и устойчивост на критичната информационна инфраструктура

Директива NIS2, официално въведена на 16 януари 2023г., дава срок на държавите-членки на ЕС да я транспонират в местното си законодателство. България ще приведе директивата в съответствие през 2026.

NIS2 е директива, а не регламент. Това означава, че законодателните й предписания са задължителни, но всяка държава-членка сама определя и изготвя свои закони, с които да постигне предписаните цели

Засегнати индустрии и предприятия:

- Енергетика
- Транспорт
- Банков сектор
- Инфраструктури на финансовия пазар
- Здравеопазване
- Питейна вода
- Отпадъчни води
- Цифрова инфраструктура
- Управление на услуги в областта на ИКТ
- Публична администрация
- Космическо пространство
- Пощенски и куриерски услуги
- Управление на отпадъците
- Производство, изготвяне и дистрибуция на химикали
- Производство, преработка и разпространение на храни
- Производство
- Доставчици на цифрови услуги
- Научни изследвания

NIS2 Обхват и изисквания

Цел и обхват на директивата

- Засилване на сигурността на мрежовите и информационни системи
- Актуална документална и технологична рамка за киберсигурност
- Задължение за докладване
- Задължение за сътрудничество на национално и европейско ниво – ЕРИКС и EU-CyCLONe

Изисквания по NIS 2

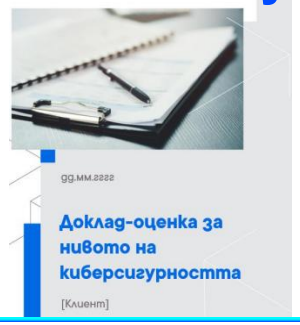
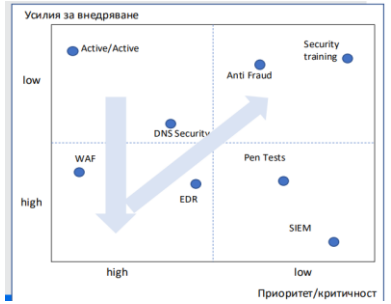
- Политики за анализ на риска и потенциалното въздействие на сигурността на информационните системи, вследствие на атака; Предприемане на проактивен, а не реактивен подход при управлението на риска
- Политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране
- Сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи
- Използването на многофакторни решения за удостоверяване на автентичността
- Сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости
- Непрекъсваемост на стопанската дейност – разработване на BCP планове и планове за възстановяване след бедствия, и управление на кризи (например: поддържане на резервни копия)

NIS2 Vivacom реализация

Времева линия

Оценка текущо състояние, изработка на препоръки, пътна карта и проект	Срок 2 до 4 седмици
Изработка политики, процеси и контролни механизми	Срок 2 до 4 седмици
Внедряване технологични и организационни мерки	Срок 6 до 18 месеца
Управление и подобрение	Постоянно

Документи, които дружеството получава

Доклад оценка	
Доклад оценка	
Пътна карта и имплементация на контролите	

Защитна стена от следващо поколениеNext Generation Firewall (NGFW)

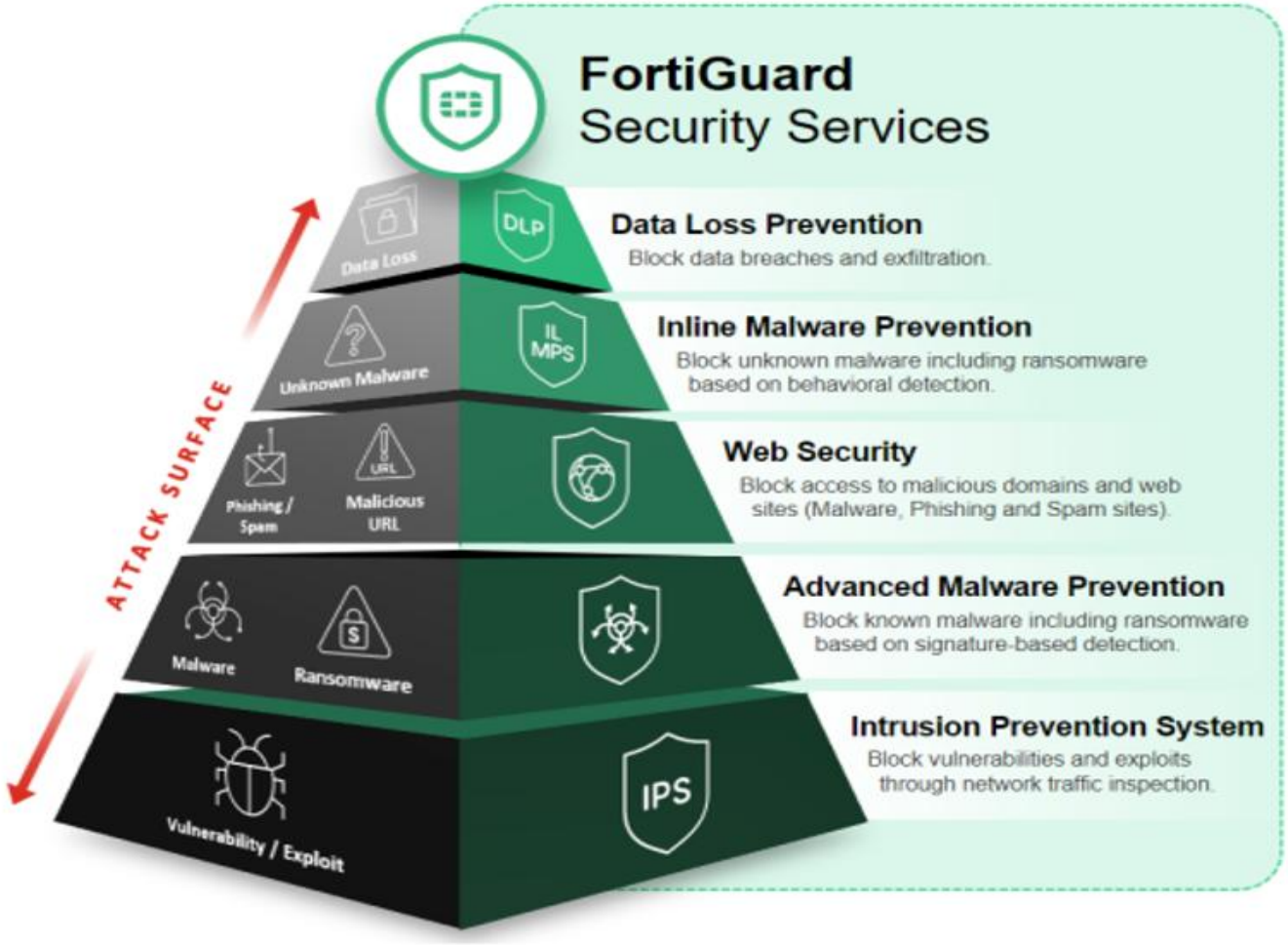
2026

Member of UNITED GROUP

Next Generation Firewall (NGFW)

NGFW надгражда стандартните защитни стени, като добавя нови услуги и защити на база динамична информация, като:

- Система за превенция на атака, чрез инспекция на трафика
- DNS филтриране на база категории
- IP репутационни правила
- URL филтриране
- WEB защита
- Email филтрация
- SSL инспекция
- Интеграция с Active Directory
- High Availability/redundancy



NIS2 и NGFW

Член от NIS2	Изискване	Как NGFW (напр. FortiGate) помага
Чл. 21 (2, т. а)	Политики за анализ и управление на риска	NGFW осигурява технически контрол за намаляване на мрежовия риск – IDS/IPS, segmentation, AV, web filter, DoS защита.
Чл. 21 (2, т. б)	Управление на инциденти и предотвратяване на инциденти	NGFW засича и блокира мрежови атаки, malware, Command&Control комуникации и аномалии в трафика.
Чл. 21 (2, т. в)	Непрекъснатост на дейността и възстановяване	NGFW поддържа High Availability (HA), failover и резервни канали за непрекъснат достъп.
Чл. 21 (2, т. г)	Откриване и реакция на инциденти	NGFW открива атаки в реално време и ги докладва към SIEM / SOC / FortiAnalyzer.
Чл. 21 (2, т. д)	Сигурност при веригите за доставки	NGFW контролира трафика между доставчици, партньори и вътрешни системи – може да прилага Zero Trust политики.
Чл. 21 (2, т. з)	Политики за криптиране и сигурен обмен на данни	NGFW осигурява SSL/TLS инспекция, IPsec VPN, SSL VPN и Zero Trust Network Access (ZTNA).
Чл. 23 (Докладване на инциденти)	Докладване на сериозни инциденти	NGFW логва и алармира при аномалии, като може автоматично да изпрати събития към FortiSIEM или национален CSIRT.

EDR (Защита чрез откриване и реагиране при заплахи на крайни точки в реално време)

2026

Антивирусна система + EDR

• Антивирусна система

Защита преди зараза и атака

- Използва сигнатури (бази данни с известни вируси).
- При сканиране сравнява файловете с тези сигнатури.
- Може да засече само познати заплахи
- Благодарение на сигнатурите и облачните бази данни, антивирусът реагира веднага при откриване на позната заплаха

EDR Защита по време на зараза и след инцидент

Детекция

Детекция на нестандартни заплахи

- Спрямо поведението
- Открива атаки
- Автоматично класифициране на заплахата

Обезвреждане

Спиране на пробив и Ransomware

- Спира злонамерени действия
- Спира загубата на данни
- Бързо време за реакция

Реакция и разследване

Пълна видимост на атаката

- Автоматизация
- Предоставя информация за разследване
- Вградени MITRE тагове

Премахване на проблема

Автоматична реакция

- Изчистване/ roll back
- Минимално прекъсване за бизнеса

NIS2 и EDR

Член от NIS2	Изискване	Как EDR (напр. FortiEDR) го подпомага
Чл. 21 (2, т. а)	Управление на риска и политики за сигурност	EDR идентифицира уязвимости и необичайно поведение на крайни точки — подпомага оценката на риска.
Чл. 21 (2, т. б)	Управление на инциденти	EDR засича и класифицира инциденти на крайни точки, стартира автоматична изолация и известяване.
Чл. 21 (2, т. г)	Откриване и реакция на инциденти	Основната функция на EDR — открива, спира и реагира на заплахи в реално време (ransomware, exploits, lateral movement).
Чл. 21 (2, т. з)	Защита на данни и обмен на информация	EDR предотвратява изтичане на чувствителна информация от крайни точки и осигурява криптиран канал за комуникация.
Чл. 23	Докладване на инциденти към компетентен орган	EDR осигурява пълна проследимост и хронология на събитията, необходими при инцидентно докладване (24–72 часа).

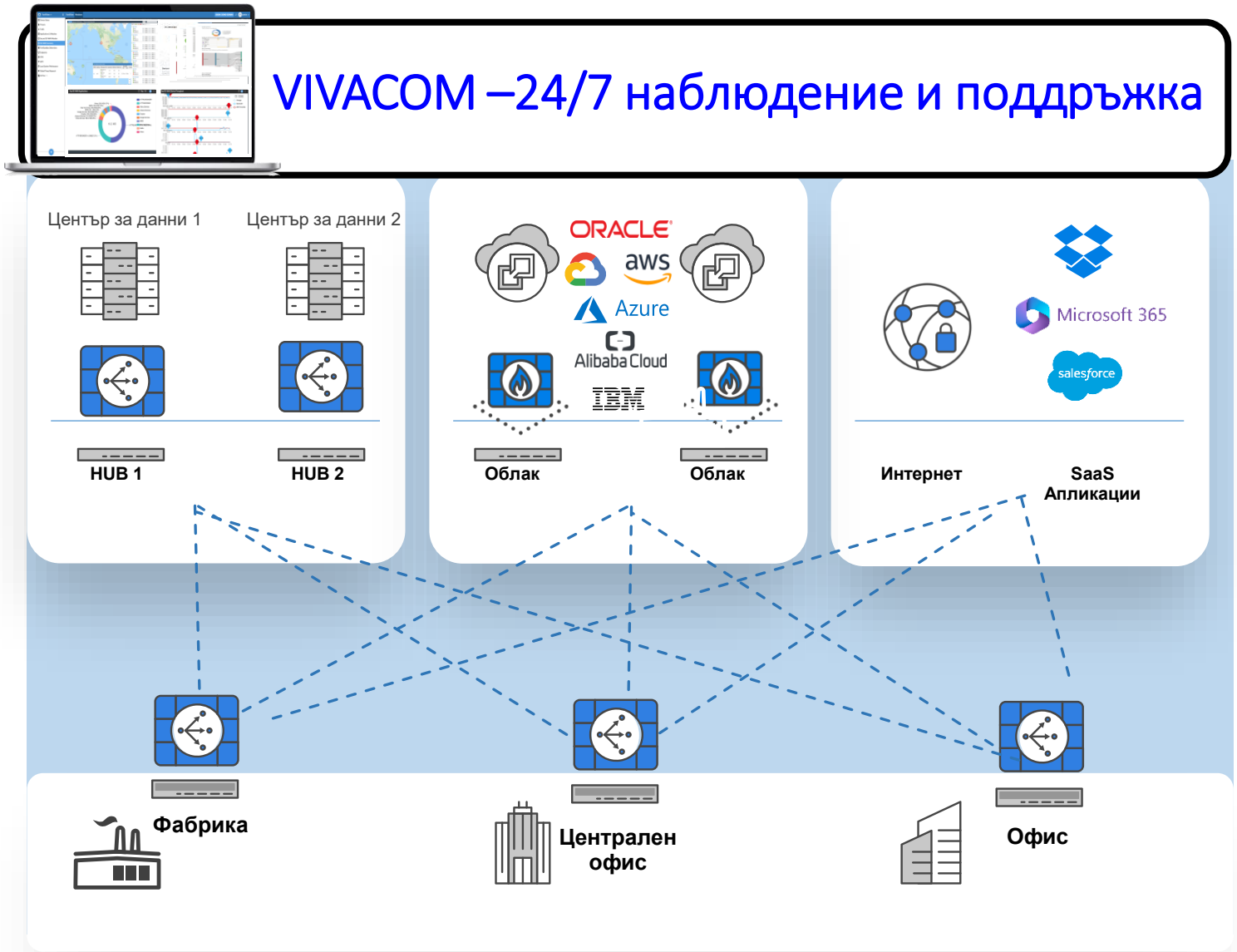
Secure SD-WAN защитена софтуерно дефинирана мрежа

2026

SD-WAN

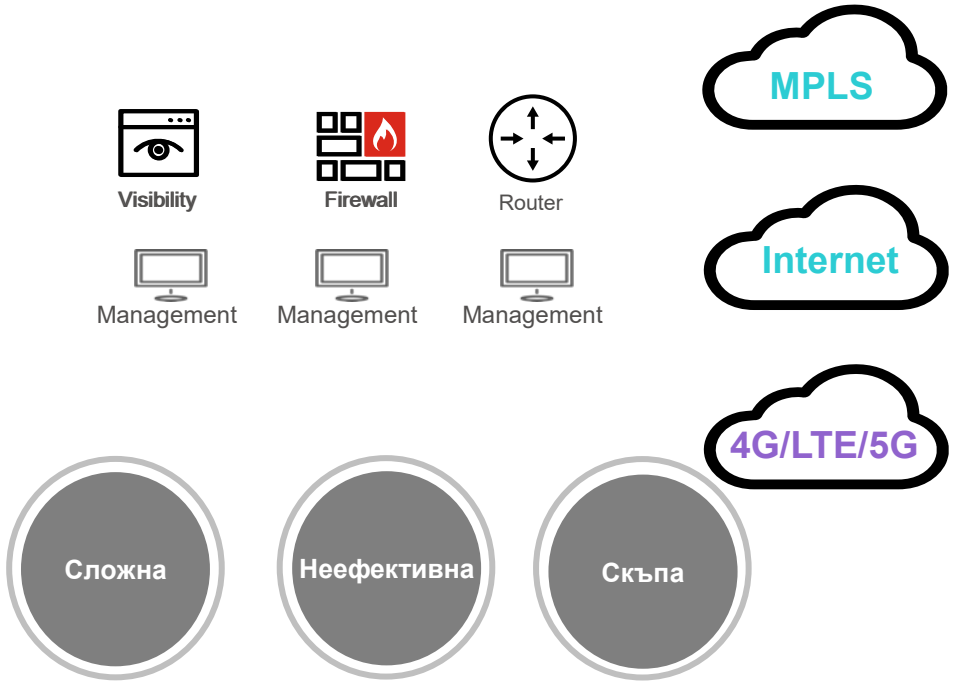
SD-WAN гъвкаво и динамично управление на мрежовия трафик на различни приложения, използвани от дадената организация.
Може да се ползва в рамките на едно автономно устройство (standalone SD-WAN) или в комбинация с overlay VPN, който осигурява свързаност между отдалечените локации на даден клиент в обща мрежа.

Архитектурата на **SD-WAN** е ориентирана към мрежовите приложения и им позволява ефективен, бърз, надежден и сигурен достъп към мрежовите услуги.

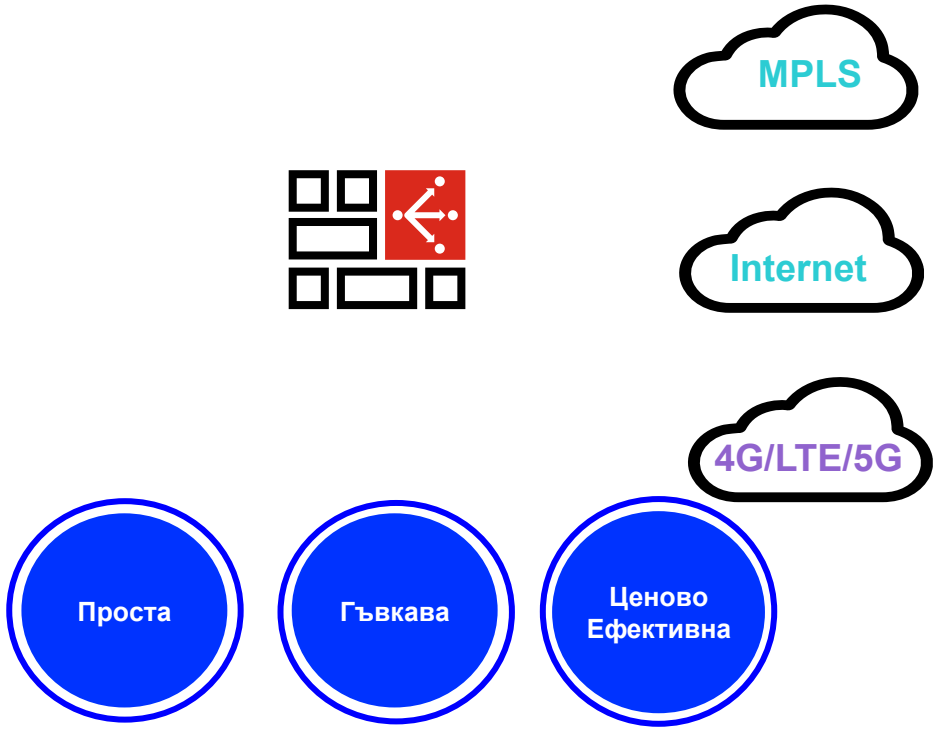


Опростена архитектура и управление

Традиционна топология

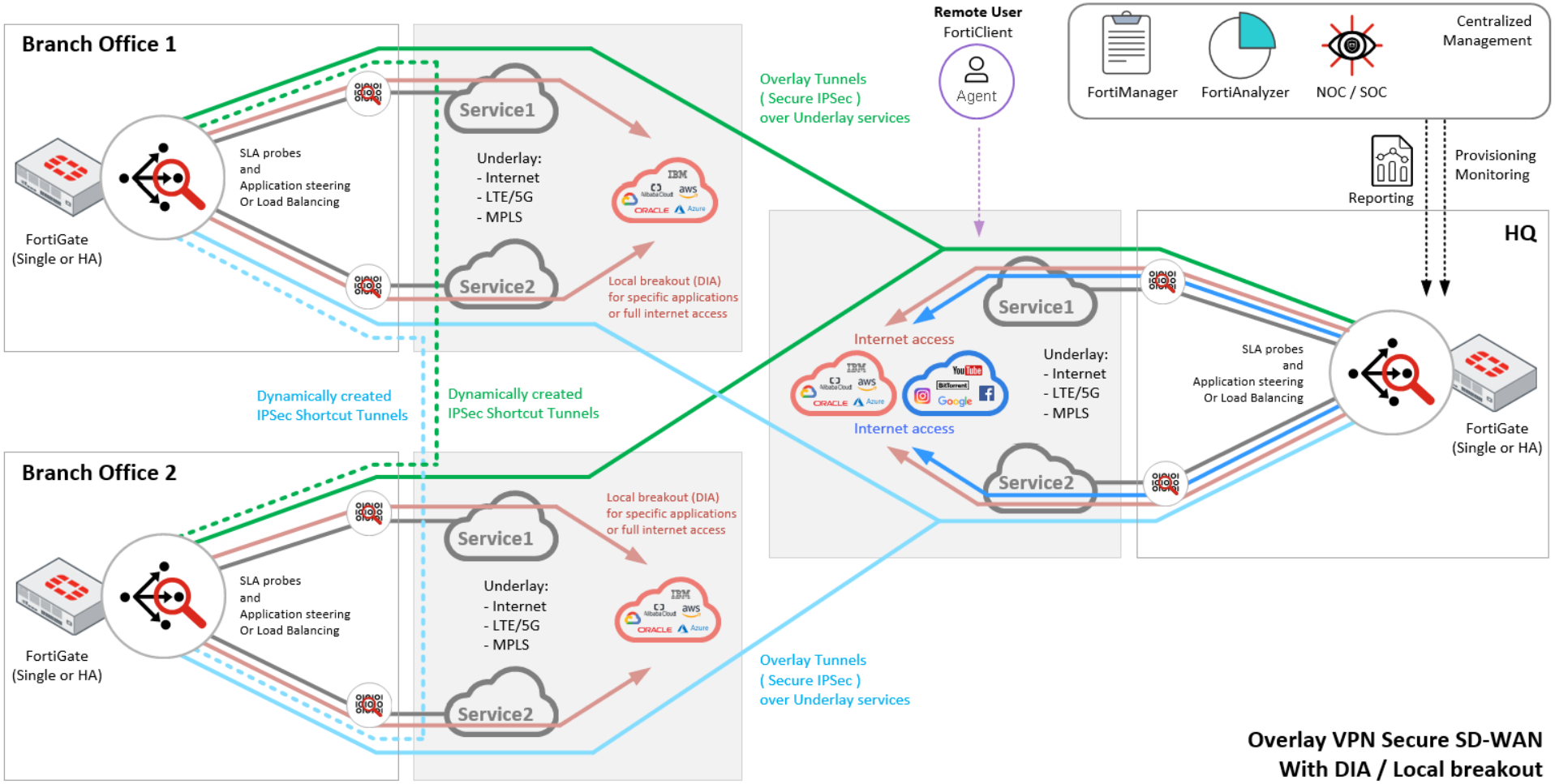


Secure SD-WAN



- Консолидирани функции в едно устройство

Overlay VPN SD-WAN with DIA



SIEM

2026

Member of UNITED GROUP

SIEM (Security information and event management)

- SIEM събира информация (логове) от множество източници (Защитни стени, сървъри, приложение и други.
- Всички данни се преобразуват в единен формат, за да могат да се сравняват и анализират.
- Системата търси **връзки между отделни събития**, които поотделно може да изглеждат безобидни, но заедно сочат към потенциална атака.
- Аларми и известия
- Дава възможност за изготвяне на доклади (могат да се използват за доказателство за съответните по NIS2)

NIS2 и SIEM

Член от NIS2	Изискване	Как SIEM помага
Чл. 21 (1–2)	Организациите трябва да прилагат мерки за управление на рискове, включително откриване и отговор на инциденти.	SIEM събира, корелира и анализира логове в реално време, за да открива заплахи и инциденти.
Чл. 21 (2, т. г)	„Откриване и обработка на инциденти, както и възстановяване след тях.“	SIEM открива инциденти чрез корелационни правила, алармира SOC екипи и предоставя forensic данни за възстановяване.
Чл. 21 (2, т. е)	„Тестове и одит на ефективността на мерките.“	SIEM събира данни, нужни за оценка и доказване на ефективност (KPI, отчети, compliance dashboards).
Чл. 23 (Докладване на инциденти)	Организациите трябва да докладват сериозни инциденти до компетентния орган.	SIEM автоматично генерира инциденти и логове, които могат да се използват при докладване (в рамките на 24/72 часа).
Чл. 26 (Водене на записи и сътрудничество)	Необходимо е централизирано управление на събитията и сътрудничество с CERT/CSIRT.	SIEM предоставя централна видимост, журнал и доказателства за взаимодействие с външни органи.
Чл. 21 (2, т. а–б)	Изискване за политики за управление на риска и непрекъснат мониторинг.	SIEM осигурява непрекъснат мониторинг, събиране на логове и индикатори за заплахи (Threat Intelligence).

Veeam Back-up as a service решение

2026

Предимства на Veeam BaaS и клиентски профил

БЪРЗО ВЪЗСТАНОВЯВАНЕ НА ДАННИ – в случай на бедствие или грешка, клиентът може незабавно да получи достъп до данните и да възстанови/активира една от запазените версии.

СИГУРНОСТ И УСТОЙЧИВОСТ НА ДАННИТЕ – Клиентските данни са защитени от неоторизиран достъп чрез криптиране и се съхраняват в инфраструктура с висока достъпност, което ги прави лесно достъпни дори в случай на бедствие.

БЕЗ ВИСОКИ НАЧАЛНИ ИНВЕСТИЦИИ - вместо големи инвестиции в хардуер, клиентът избира модел за наемане на облачно пространство за съхранение, при който плаща само за пространството, което използва за своите данни.

НЕПРЕКЪСНАТА И ГЪВКАВА УСЛУГА - клиентът може сам да определи кои данни и приложения да архивира, къде да се съхраняват и какви видове резервни копия създаваме за него и колко често. Клиентът може да промени изискванията по всяко време.

За кого е подходящо решението?

- За компании, които искат да намалят сложността и оперативната тежест от управлението на резервни копия на място.
- За организации, които искат да намалят разходите за съхранение на данни.
- За фирми, които трябва да отговарят на изискванията за съответствие и да гарантират, че политиките за архивиране в тяхната среда се прилагат по подходящ начин.
- За организации, които наскоро са претърпели прекъсване на системата или загуба на данни.
- Няма ограничение за използваната ОС

NIS2 и BaaS

Член от NIS2	Изискване	Как BaaS помага
Чл. 21 (2, т. в)	Осигуряване на непрекъснатост и възстановяване след инциденти	BaaS позволява бързо възстановяване на данни и системи след кибератаки, хардуерен отказ или човешка грешка.
Чл. 21 (2, т. а)	Управление на риска и политики за сигурност	Редовните бекъпи и тестването им са част от стратегията за управление на риска и намаляване на въздействието от инциденти.
Чл. 21 (2, т. г)	Откриване и реакция на инциденти	При атаки (например ransomware), BaaS осигурява „чисти“ копия за възстановяване и спира ескалацията.
Чл. 21 (2, т. з)	Защита на данни и сигурен обмен на информация	Backup-ите са криптирани при пренос и съхранение — гарантирайки целостта и поверителността на данните.

И още от Виваком, но не само

2026

Member of UNITED GROUP

Портфолио от решения за бизнеса

- **Частни мрежи за пренос на данни**
  Услуги и решения базирани на MPLS, предоставящи 100% изолирани от Интернет частни национални мрежи на Layer 3 и Layer 2.
- **DDoS защита**
  Пофесионална защита от непрекъснато увеличаващите се DDoS атаки, гарантираща нормална работа на бизнеса в случай на целеви опити на трети лица за блокиране на работата и предизвикване на загуби
- **WAF**
  Решения, които защитават и следят HTTP трафика, за да предпазва уеб приложенията от атаки като SQL инжекции и XSS и други специализирани атаки, които традиционните защитни стени често пропускат.
- **DLP**
  Решения за сигурност, които откриват и предотвратяват неоторизираното изнасяне на чувствителна информация извън организацията, както случайно така и целево, злонамерено от служители на фирмата
- **SOC**
  Киберспециалист под наем, наблюдаващи, откриващи, анализиращи и реагиращи всякакви събития, инциденнти и аларми с цел блокиране пробиви в инфраструктурата и системите на клиента
- **Cloud**
  Вашият виртуален Център за данни, готов за използване с лесен и удобен интерфейс за управление. Функциите Auto Scaling и Load Balancer, с които да управлявате необходимите ресурси. Заплащате само това, което сте ползвали.
- **Център за данни и DR**
  професионално място за осигуряване на надеждна и гарантирана среда за комуникационно и IT оборудване на клиент с осигурена физическа охрана, климатизация, резервирано електрозахранване

Благодарим