Persy Stinger CORE

NIS 2 READY INFRASTRUCTURE

Съфинансирано от Европейския съюз

ПРОГРАМА КОНКУРЕНТОСПОСОБНОСТ И ИНОВАЦИИ В ПРЕДПРИЯТИЯТА

Persy Stinger Core

Частна облачна система за МСП

STINGER CORE е единственото на българския пазар цялостно ИКТ решение за МСП, което в един 16U шкаф обединява разширяем хардуер от корпоративен клас, 100% open source софтуер и инженерна поддръжка от един Български производител и доставчик.
Готово за NIS 2, без лицензни такси и без време за инсталация и внедряване.

Какво е STINGER CORE

Първото на пазара цялостно решение:

- хардуер +
- софтуер +
- поддръжка

от един български доставчик,
проектирано специално за нуждите на
малките и средни предприятия.

Какво е STINGER CORE

STINGER CORE обединява изчислителен клъстер, NAS сторидж, мрежова инфраструктура, UPS, open source софтуер за виртуализация, мейл клиент, backup, firewall, с възможност за локален AI. Всичко в един 16U шкаф.

ПОТРЕБИТЕЛСКИ СЕГМЕНТ

Малки и средни предприятия

10–150 служители

СИСТЕМА

Plug and Play

Хардуер, ОС и настройки — всичко е инсталирано. Напълно готов за софтуера, с който работи бизнеса

СОФТУЕР

Без лицензионни такси

100% отворен код

ГОТОВОСТ

NIS 2-ready

10/10 мерки по чл. 21(2)

Проект BG16RFPR001-1.001-0368 · Програма КИП 2021–2027 · Съфинансирана от ЕС

За кого е създадена

Потребители

- Малки и средни предприятия - *10–150 служителя*
- Нужда от професионална ИТ инфраструктура, но без квалифициран собствен ИТ персонал, който да ги насочи към подходящо решение.
- Не искат да бъдат зависими от публични облачни услуги
- Имат регулаторни задължения (NIS 2, GDPR, ISO 27001) - или планират внедряването им.
- Обработват чувствителна или поверителна информация

Индустрии

- Юридически кантори – *поверителни клиентски данни*
- Счетоводни кантори – *поверителни клиентски данни*
- Медицински практики – *GDPR + здравна тайна*
- Производствени фирми – *ERP, MES, IoT интеграция*
- Медицински практики – *GDPR + здравна тайна*
- Финансови услуги – *регулирани финансови данни*
- Софтуерни компании – *поверителни клиентски данни*
- Архитектурни бюра – *CAD/CAM, технически данни*

Какво осигурява системата

Защитена комуникация

VLAN сегментация и нива за достъп. Отдалечен достъп в VPN чрез firewall.

ERP и бизнес процеси

Планиране, оперативно управление, отчетност

Контрол на достъпа

Физически и информационен — обекти и данни

Системи за сигурност

Подходяща за включване на видеонаблюдение, охрана, пожарна безопасност

Информационна сигурност

Репликация в реално време на данните между изчислителните възли, резервни копия и архивиране

Непрекъсваемост на услугите

При хардуерни/софтуерни повреди и отпадане на централното захранване.

Централизирано управление

Уеб-базирана мениджмънт конзола

Възможност за локален AI

On-prem (локален) асистент без зависимост от публични облачни услуги

Архитектурна концепция

STINGER CORE · 16U Rack

МРЕЖА 10G backbone · 16-port Gigabit Access · PoE Gigabit · VLAN сегментация · NGFW

HCI Cluster · Failover · Live Migration · 192 GB RAM total · min 3 TB SSD RAW

COMPUTE NODE 1
64 GB RAM
256 GB OS · 1 TB NVMe drive

COMPUTE NODE 2
64 GB RAM
256 GB OS · 1 TB NVMe drive

COMPUTE NODE 3
64 GB RAM
256 GB OS · 1 TB NVMe drive

резервирано захранване (1+1)

ДИСКОВ МАСИВ

QNAP

Backup · snapshots · репликация · RAID · до 48 TB

НЕПРЕКЪСВАЕМО ЗАХРАНВАНЕ

2k UPS

Online · 2 kVA · стабилизирано напрежение · автоизключване

Хардуер

Индустриални компоненти от корпоративен клас

Изчислителен клъстер (3 нода)

Платформа	Compact AI-ready mini embedded platform · x86-64
RAM	6 × 32 GB SODIMM (общо 192 GB)
Системен диск	3 × 256 GB SSD
Диск за данни	3 × 1 TB SSD (разпределено съхранение)
Захранване	550 W · резервирано (1+1)
Роля	Виртуализация · контейнери · възможност за локален AI

Дисков масив

Модел	QNAP (1U rackmount)
RAM	8 GB DDR4 (надграждаема до 16 GB)
SSD	3 × 2 TB
HDD (опция)	до 4 × WD 12 TB (~48 TB RAW)
Функции	Резервни копия · snapshots · репликация
Протоколи	SMB · NFS · iSCSI

192 GB	3 TB RAW	~48 TB	3-нод
RAM на клъстера	SSD на клъстера	Дисков масив с HDDs	HCI failover

Софтуерен пакет с отворен код

Без първоначални лицензни такси · без vendor lock

- ВИРТУАЛИЗАЦИЯ
- УПРАВЛЕНИЕ НА КОНТЕЙНЕРИ
- УПРАВЛЕНИЕ НА КЛИЕНТСКИ УСТРОЙСТВА
- ДИСТАНЦИОННО НАБЛЮДЕНИЕ
- МНОГОФАКТОРНА АВТЕНТИКАЦИЯ
- ОФИС ПАКЕТ
- BACKUP
- NGFW (ЗАЩИТНА СТЕНА)
- ВЪЗМОЖНОСТ за ЛОКАЛЕН AI

Ключови параметри на системата

3
изчислителни нода

192 GB
RAM на клъстера
6 × 32 GB SODIMM

2.25 TB
SSD на клъстера
OS + разпределен сторидж

2.5 Gbit
вътрешна мрежа
Up to 10Gbps + 16-port 1G

100%
open source софтуер
0,36 m² подова площ

1 Gbps port
за връзка с интернет

2 kVA
online UPS

NIS 2 10 / 10
NIS 2 чл. 21(2) мерки
техническо покритие

16U
rack капацитет
0,36 m² подова площ

01

ПРЕДИМСТВО

Завършена система

STINGER CORE доставя цялата ИТ инфраструктура като един продукт — изчисления, съхранение, мрежа, захранване, rack, back up и софтуер.

1. **Един договор, един доставчик, без допълнителни разходи**
   Не се налага да купувате UPS, switches или rack отделно
2. **Plug and play**
   Системата идва при потребителя напълно готова за експлоатация. Без нужда от допълнителна инсталация. Само включваш в електрическата мрежа.
3. **Без необходимост от назначени собствени IT специалисти**
   Наблюдението, конфигурирането на достъпа се прави от производителя
4. **Възможност за разширение**
   Предвидено място в рака за разширение - осъществява се от производителя
5. **Забележителна производителност за вложените средства (price / performance)**
   Най-много резултат (ефект) за вложените пари
6. **Уникално ниска обща цена за притежание (total cost of ownership)**
   Ниски първоначални и оперативни разходи за целия експлоатационен период

02

ПРЕДИМСТВО

Гарантирана информационна сигурност

Сигурността не е добавен модул — тя е вградена в архитектурата на хардуер и софтуер от самото начало.

1 **Next Generation FireWall (NGFW)**

периметрова защита, IDS/IPS, VPN (OpenVPN/IPsec/WireGuard)

2 **Multi-factor authentication**

passkeys/WebAuthn за всички достъпи

3 **VLAN сегментация + snapshots + immutable backup**

мрежова изолация и защита от ransomware

PERSY Stinger CORE · NIS 2 READY INFRASTRUCTURE

Непрекъсваемост на процесите

03

ПРЕДИМСТВО

ПРЕДИМСТВО

Една повреда не спира бизнеса — резервираността е заложена във всеки слой на системата.

1 **Failover клъстер**

3 изчислителни нода — натоварването се прехвърля автоматично

2 **Online UPS 2k**

защита от отпадане на захранването, стабилизиране на напрежението

3 **Дистрибутиран RAID**

Реална репликация на данните

04

ПРЕДИМСТВО

Енергийна ефективност

Компактна архитектура — производителност при минимално потребление.

1

3 изчислителни нода

Всеки с процесор с вграден NPU (Neural Processing Unit) специализиран чип, за оптимизация и ускоряване на AI операции (разпознаване и обработка на изображения и видеа, глас, обекти, мейл асистент, и т.н.) с ниска консумация на енергия

2

16U шкаф · 0,36 m²

Малка подова площ и обем

3

Естествена вентилация

без нужда от специализирано охлаждане, работи в офис среда

05

ПРЕДИМСТВО

Надеждна поддръжка

ПЕРСИ е инженерният екип, който е проектирал и асемблирал системата. Поддръжката се извършва от хората, които я познават най-добре.

1 **Сертифицирани процеси**

ISO 9001 · ISO 14000 · ISO/IEC 27001 · ISO/IEC 20000-1 · NATO AQAP 2110

2 **Поддръжка от производителя**

локален екип · бърз отговор · без езикови бариери и часови зони

3 **Open source предимство**

без зависимост от чужд вендор за лицензии или ъпдейти

Възможности за разширение на системата (на ниво индивидуална поръчка)

- Добавяне на още 2 изчислителни клъстера от по 3 нода
- Разширение до 8 TB дисково пространство във всеки нод
- Разширение на оперативната памет до 96 GB за всеки нод
- Добавяне на допълнителни батерии към UPS
- Добавяне на устройство за реална работа с AI модели
- Добавяне на допълнителен access switch
- Добавяне на допълнителен WIFI access point за безжичен достъп
- Възможност за надграждане на дисковия масив до 312 TB RAW

Съответствие с 10-те мерки на NIS 2

STINGER CORE пряко покрива 6 мерки, подкрепя останалите 4

#	Мярка по чл. 21(2)	Как STINGER CORE я подкрепя	Степен
a	**Анализ на риска и политики**	Централизирана регистрация на събития · одитни записи · пълна проследяемост	Подкрепя
b	**Управление на инциденти**	Мониторинг на ресурси · регистриране на инциденти · система за откриване и предотвратяване на проникванията · уеб конзола	Пряко
c	**Непрекъсваемост и backup**	Резервни копия · снапшоти · непрекъсваемо захранване · клъстерна отказоустойчивост	Пряко
d	**Сигурност на веригата на доставки**	Единен местен доставчик · изцяло отворен код · проследяемост на уязвимости	Подкрепя
e	**Придобиване / развитие / уязвимост**	Централизирано управление · виртуализация · контейнеризация · проследяване на уязвимости	Пряко
f	**Оценка на ефективността**	Централизирана регистрация на събития · одитни пътеки · уеб метрики	Подкрепя
g	**Стандарти за киберсигурност и обучение**	Best practices · PERSY обучение като услуга	Подкрепя
h	**Криптография и шифроване**	Криптирани комуникации · VPN · шифроване на дискове	Пряко
i	**HR / достъп / asset management**	Централизирано управление на потребители · инвентаризация на устройства · одитни записи за всеки достъп	Пряко
j	**MFA и защитени комуникации**	Многофакторна автентикация с passkey/WebAuthn · криптирана поща · VPN	Пряко

Обобщение: пряко покрива 6 от 10 мерки (b, c, e, h, i, j) и подкрепя останалите 4 от 10 (a, d, f, g) чрез предоставянето на технически инструменти, върху които организацията изгражда своите политики и процедури.

Проект BG16RFPR001-1.001-0368 · Програма КИП 2021–2027 · Съфинансирана от ЕС

Каква е отговорността на клиента по NIS2

Разграничение между техническите контроли и организационните мерки

✓ STINGER CORE предоставя

Технически контроли:

- ✓ Защитна стена и сегментация
- ✓ MFA и passwordless автентикация
- ✓ Шифроване и VPN канали
- ✓ Backup, snapshots и репликация
- ✓ Online UPS и failover клъстер
- ✓ Централизиран вход за достъп
- ✓ Patch management
- ✓ Audit trails за всеки достъп
- ✓ Възможност за локален AI без нужда от публична облачна платформа

⚠ Отговорност на клиента

Организационни мерки:

- ○ Политики за информационна сигурност
- ○ Политика за управление на инциденти
- ○ Роли и отговорности по сигурността
- ○ Обучение на персонала *
- ○ Процедури за отчитане на инциденти
- ○ Анализ на риска за конкретни данни
- ○ Договори с подизпълнители (supply chain)
- ○ Обработка на класифицирана информация
- ○ Управление на промените (change mgmt)

** PERSY предлага обучение и подкрепа при изготвяне на политики като отделна консултантска услуга.*

Проект BG16RFPR001-1.001-0368 · Програма КИП 2021–2027 · Съфинансирана от ЕС

Три едновременни нужди на МСП

STINGER CORE адресира всичките — в един продукт

01 Технологична основа за ефективни процеси

МСП имат нужда от съвременна, професионална ИТ инфраструктура, но нямат квалифициран собствен ИТ персонал, който да ги насочи към подходящо решение.

STINGER CORE и HCI архитектурата му решават това.

02 Защита на данните

МСП имат нужда от защитени данни, без злонамерен достъп до тях, обезпечени с резервни копия и в съответствие със законовите норми.

STINGER CORE е on-premise решение, без зависимост от изнасяне към публични облачни услуги.

03 Ценова ефективност

МСП имат нужда от ниски първоначални и оперативни разходи и предвидими разходи за поддръжка.

STINGER CORE предлага ниски CAPEX и OPEX.

Свържете се с нас

Готови сме да обсъдим Вашия конкретен сценарий за внедряване

www.persy.com
sales@persy.com
070042030
гр. София 1330, ул. „Златна Добруджа" 18