infocom
TRUSTED SECURITY

СП «Інфоком»
вул. Володимирська, 8
Київ, 01001, Україна
тел.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

# infoGuard

## Багаторівневий захист периметру мережі

infocom.ua

2024

## ІНФОРМАЦІЙНА БЕЗПЕКА

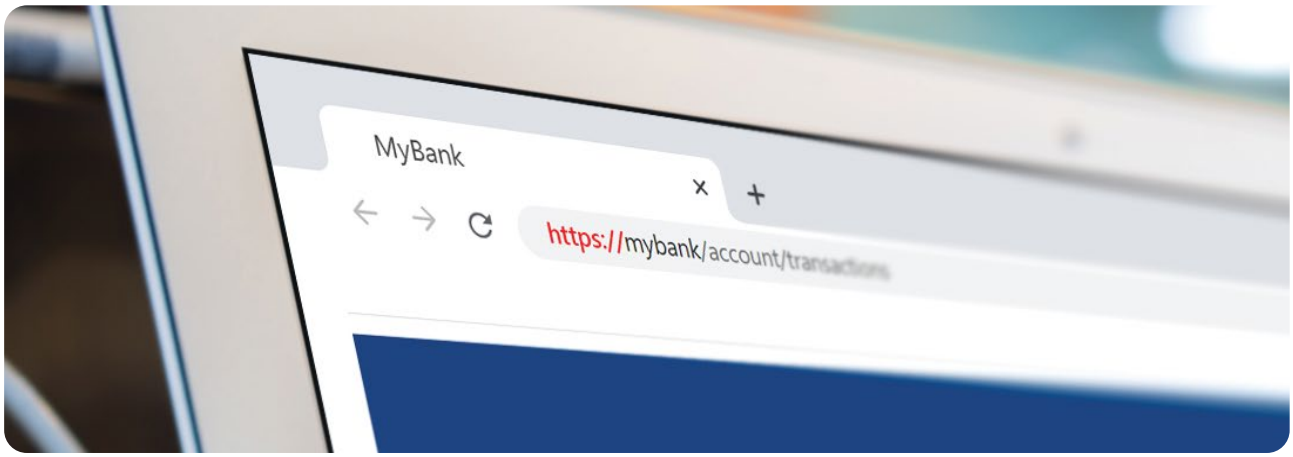
Робота державної чи фінансової установи, великого або малого бізнесу, навчального чи медичного закладу нерозривно зв'язана з використанням цифрових інформаційних технологій, які, в значній мірі, дозволяють спростити, впорядкувати, автоматизувати та значно підвищити ефективність усіх наявних організаційних, фінансових, виробничих або будь-яких інших процесів. Будь-яке несанкціоноване втручання у роботу відповідної інформаційної інфраструктури збоку зловмисників або недоброчесних конкурентів може не тільки тимчасово зупинити важливі робочі процеси але й через виток конфіденційної внутрішньої інформації призвести до значних репутаційних або фінансових втрат.
Послуги Infocom з інформаційної безпеки покликані мінімізувати будь-які ризики несанкціонованого доступу у вашу інформаційну інфраструктуру та забезпечити її надійне та безперервне функціонування завдяки всебічному захисту як зовнішнього так і внутрішнього периметру.

# infoGuard

web-сторінка послуги

## БАГАТОРІВНЕВИЙ ЗАХИСТ ПЕРИМЕТРУ МЕРЕЖІ

infoGuard — це перша лінія захисту вашої інформаційної інфраструктури. Це важливий елемент, який запобігає несанкціонованому сторонньому втручанню у корпоративну мережу, контролює та відстежує діяльність співробітників, приймає, відхиляє або припиняє доступ ззовні водночас дозволяючи вам бути гнучкими та динамічними у виконанні ваших бізнес-задач.




Широке використання безпечного протоколу передачі даних HTTPS, який унеможливлює «прослуховування» мережевого з'єднання під час відвідування веб-сторінок різноманітних онлайн-сервісів, значно знижує ризик перехоплення приватної конфіденційної інформації третіми особами, але в той самий час приховує від звичайних систем захисту увесь потік даних між користувачем та веб-порталом. Це створює не тільки можливість проникнення всередину корпоративної мережі вірусів, шпигунського програмного забезпечення, системних моніторів, кілоґґерів та іншого шкідливого програмного забезпечення через комп'ютер співробітника, але й скриває вихідний потік даних, який може містити конфіденційну корпоративну інформацію. Оскільки об'єм трафіку з використанням протоколу HTTPS, за статистикою, складає понад 80% від загального, аналіз системами безпеки зашифрованих даних стає однією з основних складових сучасного інформаційного захисту. Послуга infoGuard дозволяє перевіряти зашифровані дані, виступаючи

своєрідним посередником між користувачами та веб-порталами, таким чином значно знижуючи ризики проникнення шкідливого ПЗ у корпоративну мережу завдяки аналізу на наявність загроз усього, без виключення, вхідного та вихідного трафіку.

Основною метою сучасних кіберзлочинців є викрадення конфіденційної корпоративної та особистої інформації через вторгнення у мережу завдяки наявним вразливостям встановленого обладнання та програмного забезпечення. Система запобігання вторгненням сервісу infoGuard постійно аналізує всі зовнішні запити, що дозволяє попередити можливі атаки та спричинені цим негативні наслідки. Окрім аналізу зовнішніх запитів, infoGuard має гнучку систему внутрішнього контролю, яка завдяки аналізу вихідних даних значно зменшує вірогідність витоку конфіденційної інформації, спричиненого ненавмисними, або злочиними діями співробітників компанії.

Послуга infoGuard містить функцію динамічної веб-фільтрації в режимі реального часу, яка блокує відвідування співробітниками компанії скомпрометованих, або навмисно створених ресурсів за допомогою яких злочинці отримують доступ до персональних та корпоративних даних, або завантажують шкідливе програмне забезпечення. За потребою клієнта, система дозволяє створити додаткові фільтри та закрити для перегляду співробітниками окремі сайти, або цілі категорії веб-ресурсів: із азартними іграми, онлайн переглядом фільмів, «дорослі» ресурси, тощо.

Функція контролю додатків infoGuard безперервно класифікує і оцінює трафік програм, якими користуються співробітники компанії. Система контролю дозволяє блокувати, або обмежити доступ до ризикованих програм, цілих категорій програм, оптимізує використання пропускної здатності у вашій мережі, встановлюючи пріоритети програм чи повністю блокуючи небажаний трафік. Наприклад, infoGuard дає можливість заблокувати перегляд відео чи прослуховування аудіофайлів у соціальних мережах, залишаючи при цьому доступ до світлин та дописів.

Розгортання та спосіб підключення послуги infoGuard залежить від того чи є замовник користувачем послуг Infocom, а саме телекомунікаційних послуг infoSDWAN чи infoVPN, або послуг з доступу до мережі «Інтернет». В цьому разі підключення послуги займає мінімальний проміжок часу, а усі комутаційні роботи та відповідне налаштування відбуваються всередині Infocom без додаткових робіт та налаштування на боці замовника (крім встановлення на робочі комп'ютери сертифікатів infoGuard для аналізу зашифрованого трафіку). Якщо замовник не є користувачем вищезгаданих послуг Infocom на боці замовника або створюється GRE-тунель, який спрямовує увесь вхідний трафік на обладнання infoGuard яке встановлене у Infocom, або замовнику послуги надається окрема кількість устаткування яке встановлюється у кожній кінцевій точці та здійснює перевірку трафіку безпосередньо на боці замовника.

У рамках послуги infoGuard спеціалісти Infocom можуть взяти на себе функції адміністрування клієнтського устаткування, якщо у вас немає власної команди з інформаційної безпеки. Це означає, що наша команда забезпечить ефективний моніторинг та захист ваших мереж та систем від зловмисних атак та інших загроз 24/7 використовуючи ваше обладнання.

## Послуга infoGuard це:

- Зниження ризиків порушення діяльності вашої компанії
- Оптимізація ваших витрат на забезпечення кіберзахисту завдяки відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього
- Безпечне користування мережею «Інтернет»
- Можливість оперативно змінювати кількість підключених до сервісу філій/відділень, як у бік збільшення, так і у бік зменшення.
- Моніторинг і контроль атак та інцидентів 24x7x365
- Залучення фахівців Infocom без необхідності у додатковому навчанні власних
- Підтримка 24x7x365

infocom
TRUSTED SECURITY