infoGuard

Багаторівневий захист периметру мережі та даних

infocom
TRUSTED SECURITY

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.

Основними складовими послуги infoGuard є:

• Антивірус

Сканування трафіку забезпечує захист від шпигунського та шкідливого ПЗ, включаючи захист від троянів, фішінг-програм, системних моніторів, кейлоггерів, а також захист від рекламного програмного забезпечення.

Оскільки сьогодні більш ніж 80% мережевого трафіку зашифровано, здатність його розшифровувати та перевірити на на явність загроз є основним елементом сучасного захисту. Сервіс infoGuard надає таку можливість* та не просто тільки тому, що цей значний відсоток від всього корпоративного трафіку потребує обов'язкової перевірки, а й тому, що це додатково дає змогу набагато підвищити ефективність ключових функцій (наприклад: контроль «обхідних маневрів», контроль та керування роботою програм, блокування чи обмеження небажаних програм).

• Розширений захист від загроз (Advanced threat protection)

Наше рішення включає в себе кілька комплексних модулів перевірки джерел даних про загрози та варіантів захисту від невідомих загроз, а також контроль за активністю ПЗ клієнта.

Аналіз файлів за допомогою зовнішнього хмарного сервісу (Sandbox), у тому числі з використанням динамічних сигнатур для потенційних загроз нульового дня. Інспекція SSL та TLS шифрованого трафіку профілями системи запобігання вторгнень, контролю додатків, антивірусу, веб фільтрації тощо. Блокування Botnet мереж за допомогою найбільшої глобальної репутаційної бази даних.

• Система запобігання вторгнень (IPS)

Забезпечення захисту за допомогою бази даних вразливостей та кількісного аналізу. Розпізнавання і блокування TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding.

• Контроль додатків

Багато програм мають суттєво різні функції, що представляють різні рівні ризиків і цінності як для користувача, так і для організації. Система безпеки безперервно класифікує і оцінює трафік, функції програм та спостерігає за їх змінами. При кожній зміні поведінки програми, система перевіряє її на відповідність налаштованим політикам безпеки.

Визначення та керування програмами, що використовують одне і те ж з'єднання - є важливою особливістю, оскільки на сьогодні клієнт працює з багатьма "платформами" (Google, Facebook, Microsoft, Salesforce, LinkedIn, чи Yahoo), де розробники додатків інтегрують багато різних програми, які часто мають дуже різні потенціали ризику та бізнес-цінність.

Наприклад, Gmail не тільки надсилає листи, а й має можливість створити сесію Google Talk прямо з інтерфейсу Gmail. Ці програми є принципово різні, але наша система безпеки визначає кожну та застосовує окрему політику, згідно з рекомендаціями та побажаннями замовника.

Розробники ПЗ більше не дотримуються стандартного поєднання портів та протоколів; все більше і більше додатків здатні працювати на нестандартних портах (наприклад, програми миттєвих повідомлень, peer-to-peer обмін файлами, або VoIP). Крім того, розробники ПЗ все більше докладають зусиль, щоб змусити програми працювати через нестандартні порти (наприклад, MS RDP, SSH). У такому випадку, для забезпечення виконання специфічних правил, система захисту класифікує трафік за програмою (весь час на всі порти), що дає можливість гнучко контролювати правила роботи і поведінку кожної програми.

Також наше рішення підтримує виявлення трафіку додатків за допомогою протоколу HTTP/2 та можливість блокувати QUIC-трафік, щоб браузер автоматично повертався до HTTP/2 + TLS 1.2.

• Контент-фільтр

Функція включає: динамічну веб-фільтрацію в режимі реального часу за допомогою хмарного сервісу БД веб-ресурсів з можливістю створення статичних фільтрів, можливість безпечного пошуку, а саме прозора вставка параметрів SafeSearch в запити, підтримка Google, Yahoo!, Bing, YouTube Education Filter тощо, створення локальних категорій веб ресурсів на потребу клієнта, запобігання використання проксі, фільтрація Java Applet, ActiveX, cookie, блокування HTTP post дій, журналювання пошукових запитів, рейтинг зображень по URL, блокування HTTP redirects, налаштування квот на веб-перегляд.

• Запобігання витоку даних

Сервіс infoGuard забезпечує високий рівень безпеки завдяки багаторівневой фільтрації трафіку, яка колосально зменшує вірогідність витоку конфіденційної інформації! Сервіс надає можливість фільтрації повідомлень, файлів та має додаткові налаштування.

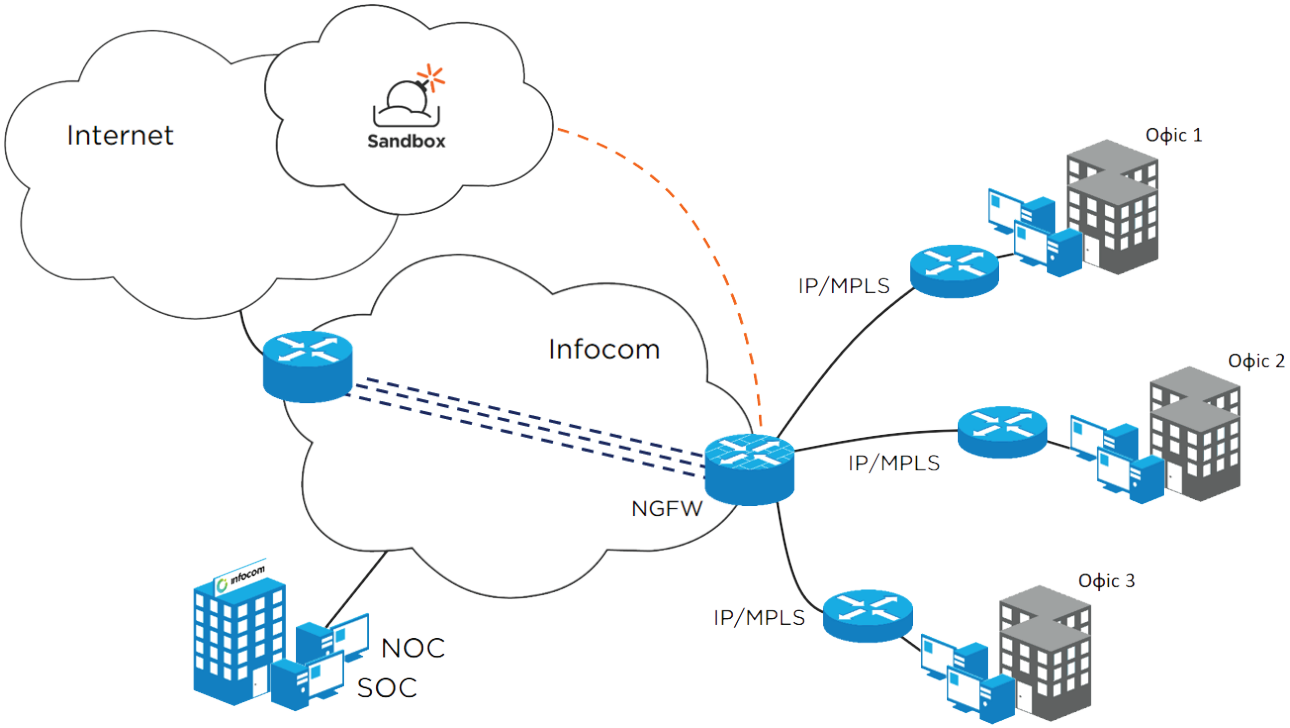
Фільтрація повідомлень (протоколи): HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP.
Фільтрація файлів (протоколи): HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP.
Налаштування фільтрації: розмір, тип файлу, водяний знак.

• Захист робочих місць

Робочі місця дуже часто стають мішенями різного роду кібератак. Нещодавне дослідження показало, що 30% атак було скоєно за допомогою установки шкідливого ПО в кінцевих точках. Шляхом встановлення агентів з інтегрованим засобами відстеження, контролю та запобігання розповсюдження, ми значно посилюємо безпеку робочих місць. Функції виявлення, моніторингу та оцінки загроз, яким піддається кінцева точка, дозволяють пом'якшити ризики і знизити рівень незахищеності.

Розгортання сервісу

Сервіс infoGuard може бути запущений як на базі власної IP/MPLS мережі Інфокому, так і на підключеннях від інших провайдерів.



На все обладнання та програмне забезпечення, яке ми використовуємо, маємо в наявності **експертний висновок Державної служби спеціального зв'язку та захисту інформації України** щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні