Trellix

# Trellix Endpoint Security (HX)

**Trellix Endpoint Security (HX) захищає від сучасних кібератак, використовуючи модель ешелонованого захисту.**

Модульна архітектура Endpoint Security (HX) поєднує стандартні механізми та завантажувані модулі для захисту, виявлення та реагування, а також управління безпекою кінцевих точок.

Endpoint Security можна розгорнути як локальний апаратний пристрій, який захищає до **100 000 кінцевих точок,** віртуальний пристрій або у хмарі.

## Запобігайте кібератакам на кінцевій точці

- Ідентифікуйте поведінку зловмисників, їхні тактики, техніки та процедури.
- Аналізуйте оперативну пам'ять — без завантаження образів пам'яті — для виявлення прихованих шкідливих програм.

## Виявляйте шкідливі програми та інші ознаки компрометації кінцевих точок

- Перевірте тисячі кінцевих точок на предмет компрометації, включно зі шкідливим ПЗ і нестандартними діями.
- Організуйте безпечне дистанційне розслідування у будь-якій мережі без зайвої авторизації.
- Збирайте цільові криміналістичні дані за допомогою інтелектуальної фільтрації, щоб повертати тільки ті дані, які вам потрібні.

trellix@bakotech.com // trellix.bakotech.com

# Trellix Endpoint Security (HX)

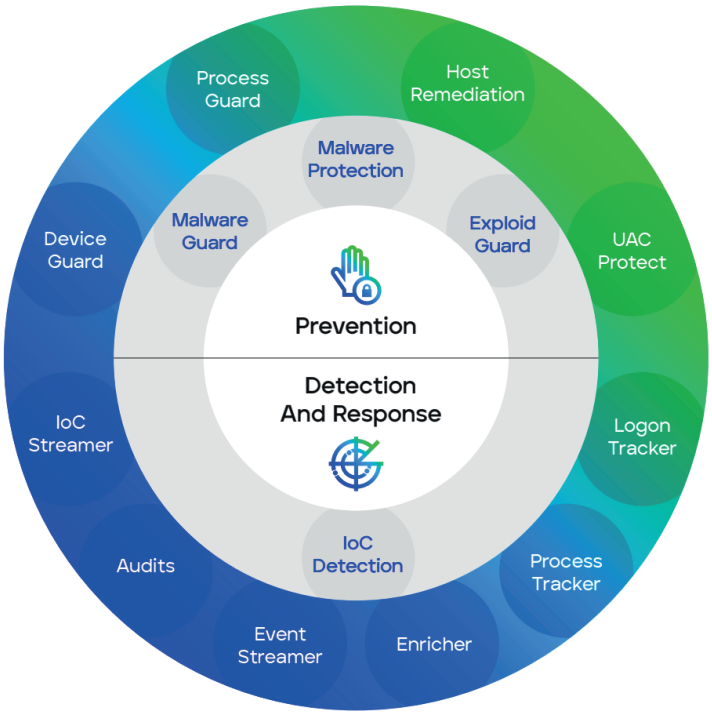
## Швидше реагуйте на інциденти, пов'язані з безпекою кінцевих точок

- Скористайтеся можливістю віддаленого підключення до командної оболонки кінцевих точок для аналізу та усунення загроз.
- Інтегруйтеся з іншими системами виявлення, щоб автоматизувати сортування хостів із підозрілою активністю.
- Автоматично збирайте дані та аналізуйте підозрілу активність на основі попереджень, що генеруються вашим SIEM, системою тікет-менеджменту або іншими програмами.
- Скористайтеся відкритими IOC, щоб редагувати та публікувати власні IOC.

### Навіть з найкращим захистом вторгнення неминучі.

Щоб забезпечити реагування, що мінімізує збої в роботі, Endpoint Security (HX) передбачає можливості виявлення та реагування на кінцевих точках, що ґрунтуються на індикаторах компрометації в реальному часі (IOC), розроблених за допомогою передових фахівців. Інструменти Trellix також:

- Проводять пошук та розслідування відомих та невідомих погроз на десятках тисяч кінцевих точок за лічені хвилини
- Визначають, чи відбулася атака (і чи зберігається загроза) на конкретній кінцевій точці, а також у яких межах вона поширилася
- Визначають та деталізують вектори атаки, які використовуються для проникнення на кінцеву точку
- Встановлюють хронологію та тривалість компрометації кінцевих точок, а також стежать за перебігом інциденту



# Trellix Endpoint Security (HX)

## Особливості

- Один агент, який використовує багаторівневий захист, щоб звести до мінімуму конфігурацію та максимізувати виявлення та блокування
- Вбудована інтеграція з Trellix XDR для більшої видимості та контролю, що дозволяє повністю усунути всі загрози в організації
- Збір даних для проведення поглибленої перевірки та аналізу кінцевих точок протягом певного періоду часу
- Захист від шкідливих програм за допомогою інструментів для зміцнення безпеки, машинного навчання, аналізу поведінки, індикаторів компрометації (IOC) та видимості кінцевих точок
- Корпоративний пошук для швидкого виявлення підозрілої активності та загроз
- Повна видимість, що дозволяє службам безпеки швидко шукати, ідентифікувати та визначати рівень загроз

## КОНТАКТИ

trellix@bakotech.com

trellix.bakotech.com

Trellix | bakotech®

WE BRING SECURITY TO LIFE