Багаторівневий захист –

запорука безпеки бізнесу в реаліях сьогодення

Олександр Іллюша

Технічний директор

alex@eset.ua

Еволюція загроз

Прості
Загрози

Складні
Стійкі загрози

Цілеспрямовані
атаки

Найпоширеніші класи загроз у 2020-2021 роках

Банківське шкідливе програмне забезпечення

Програми-вимагачі

Завантажувачі та криптомайнери

Шпигунські програми та бекдори

Експлойти

Загрози для Mac

Загрози для Android

Веб-загрози

Найактивніші APT-угрупування у 2020-2021 роках

Winnti Group

Gamaredon

Turla

In(ter)ception

TeleBots

Zebrocy (Sednit)

Mustang Panda

Energetic Bear

IT-інфраструктура постійно змінюється

Розвиток технологій

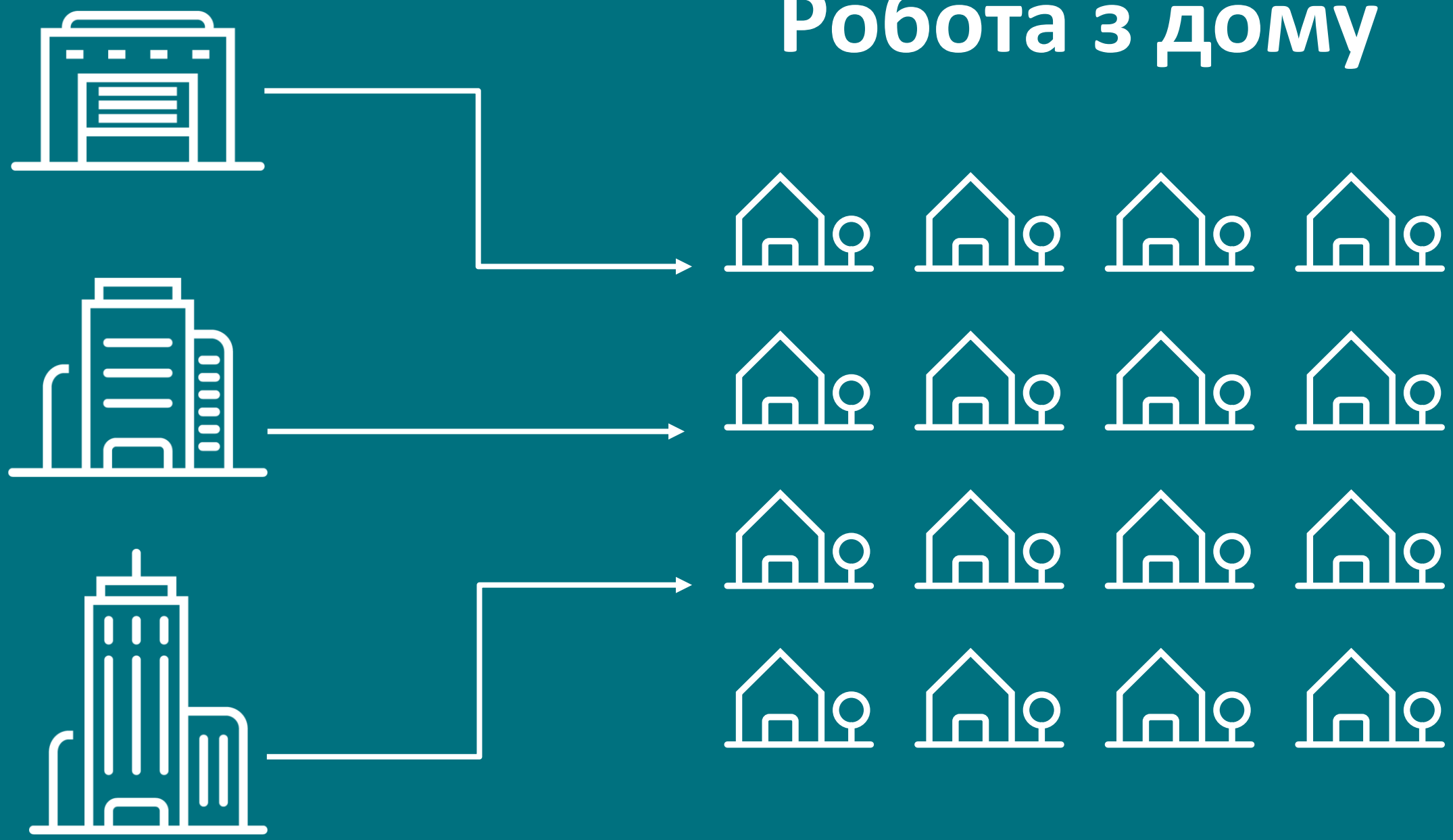
Промисловий Інтернет речей

Побутовий Інтернет речей

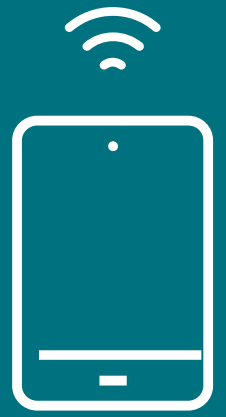
COVID-19


2020

Робота з дому

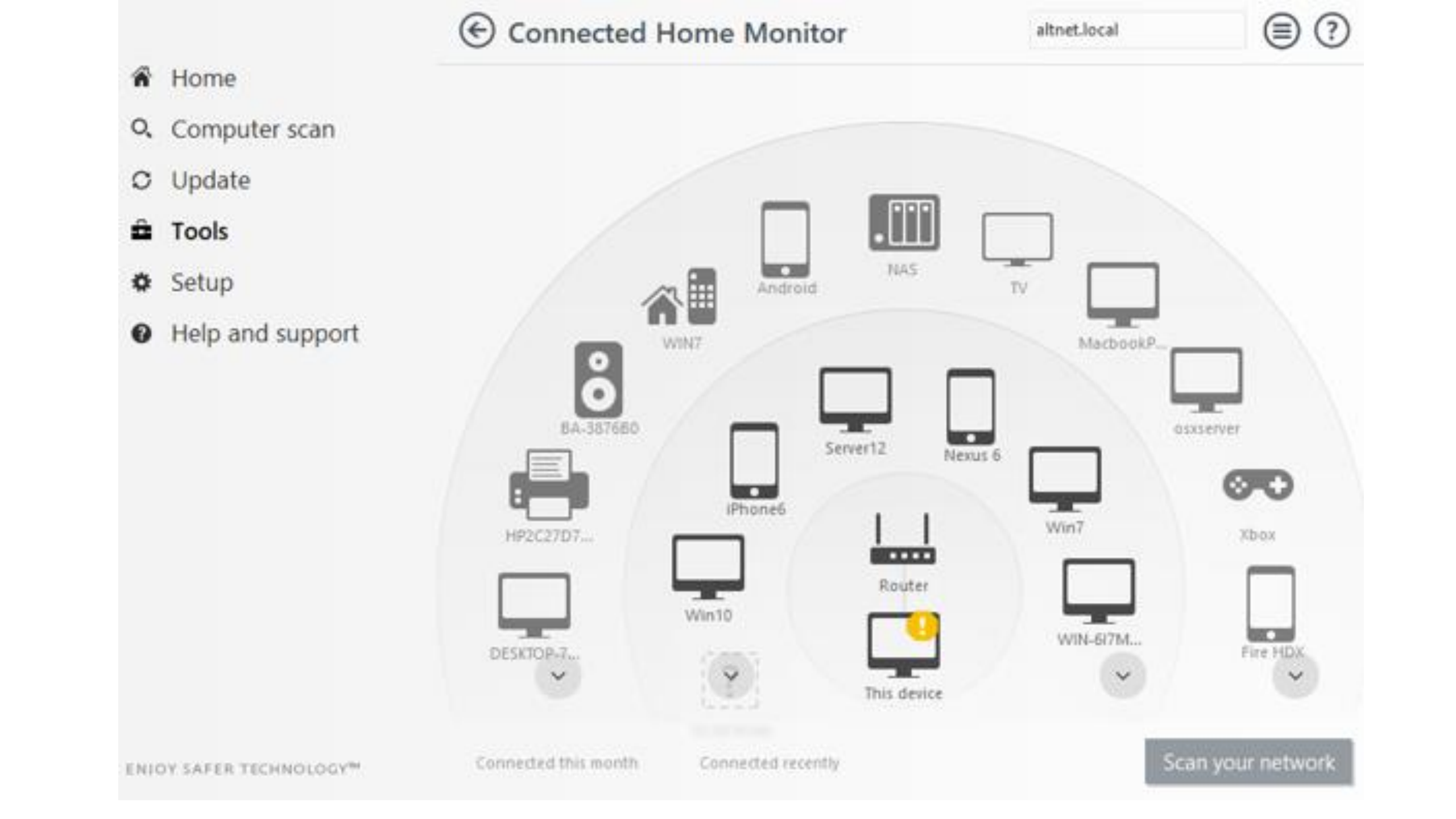




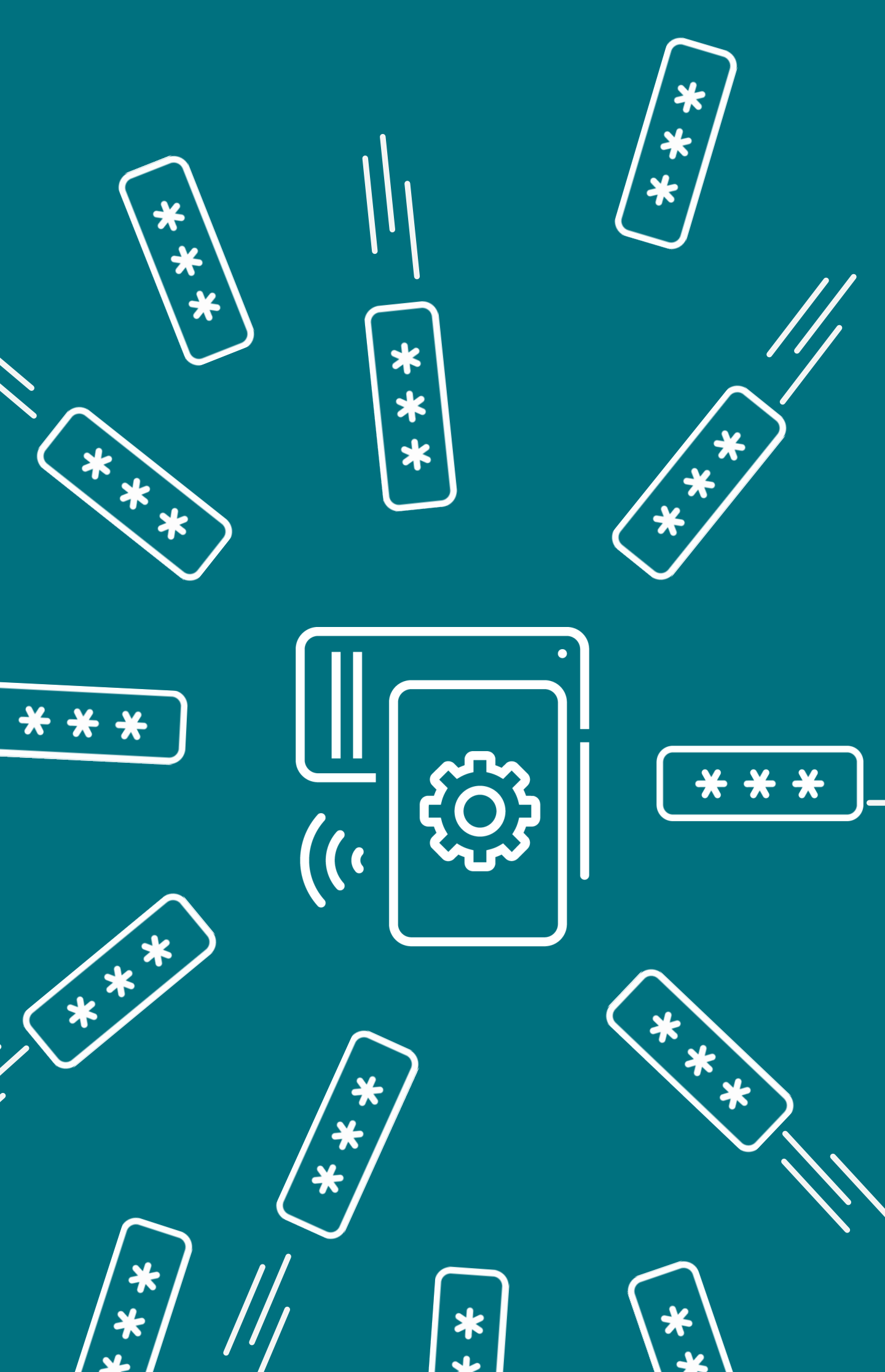


Віддалений доступ для всіх

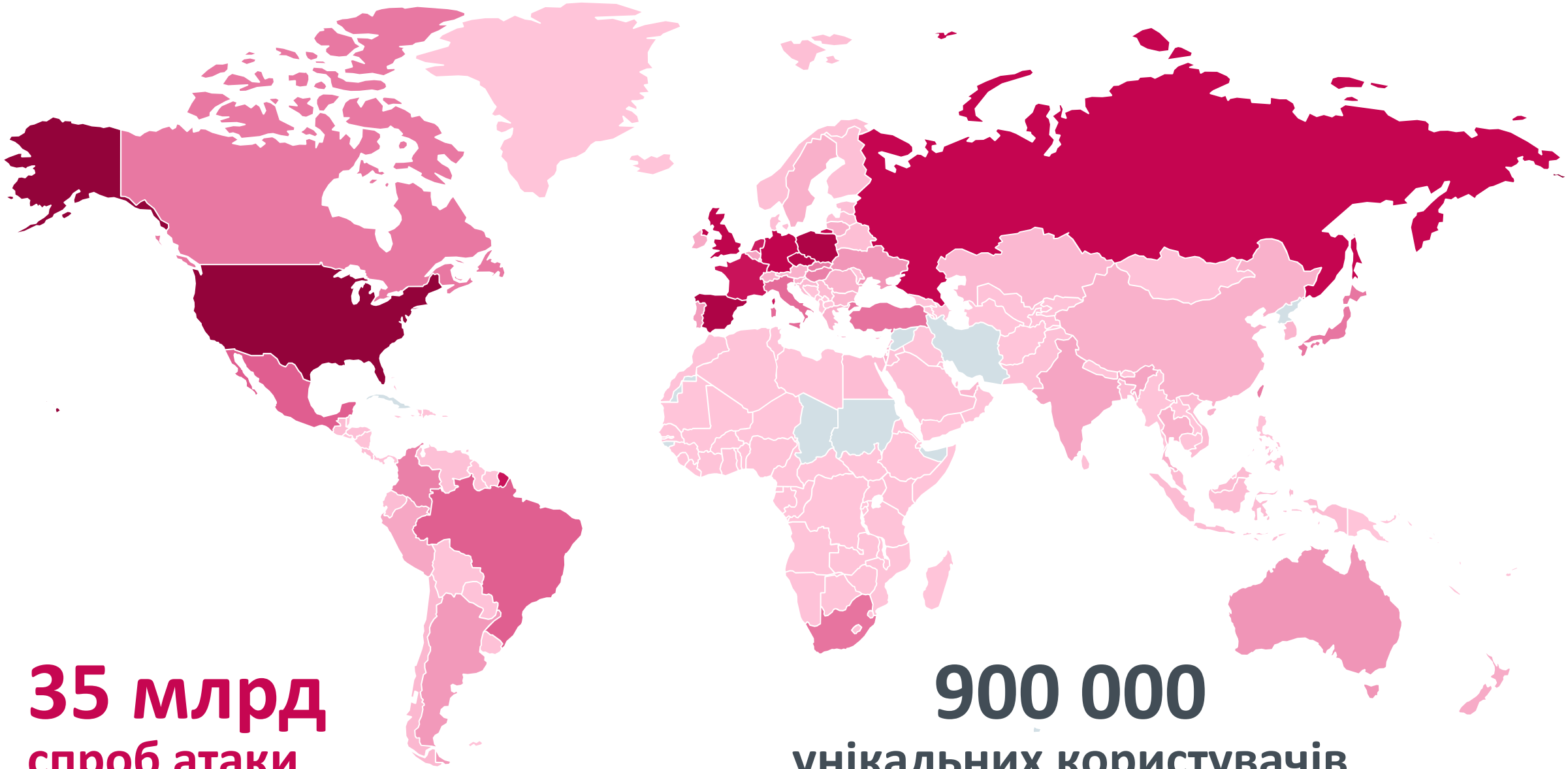




Connected Home Monitor
altnet.local
Home
Computer scan
Update
Tools
Setup
Help and support
Android
NAS
TV
WIN7
MacbookP...
8A-387680
Server12
Nexus 6
osxserver
iPhone6
HP2C27D7...
Win7
Xbox
Router
Win10
DESKTOP-7...
WIN-6I7M...
Fire HDX
This device
Connected this month
Connected recently
Scan your network
ENJOY SAFER TECHNOLOGY™

Атака підбору паролів через RDP

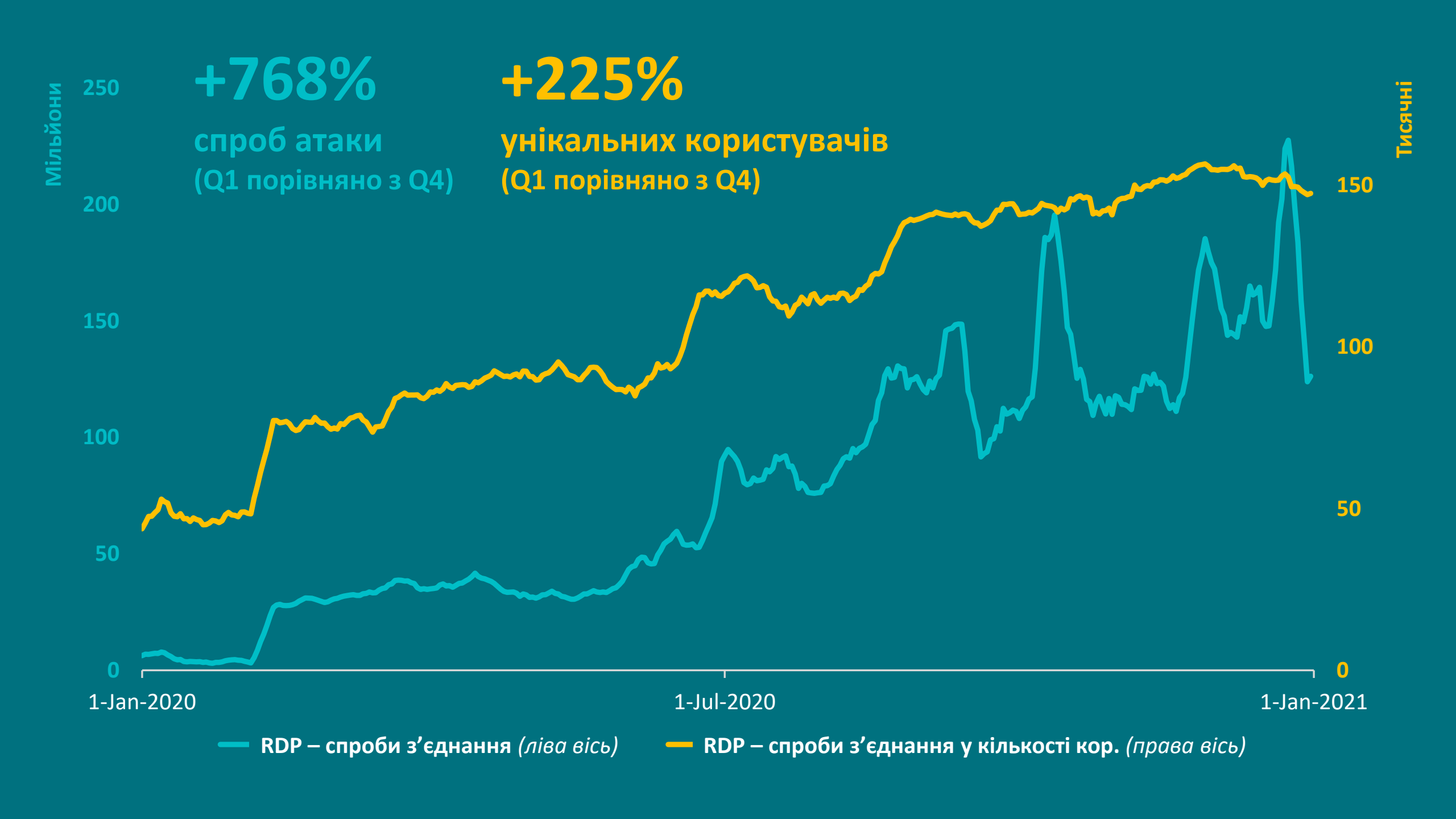


RDP – атака підбору паролів



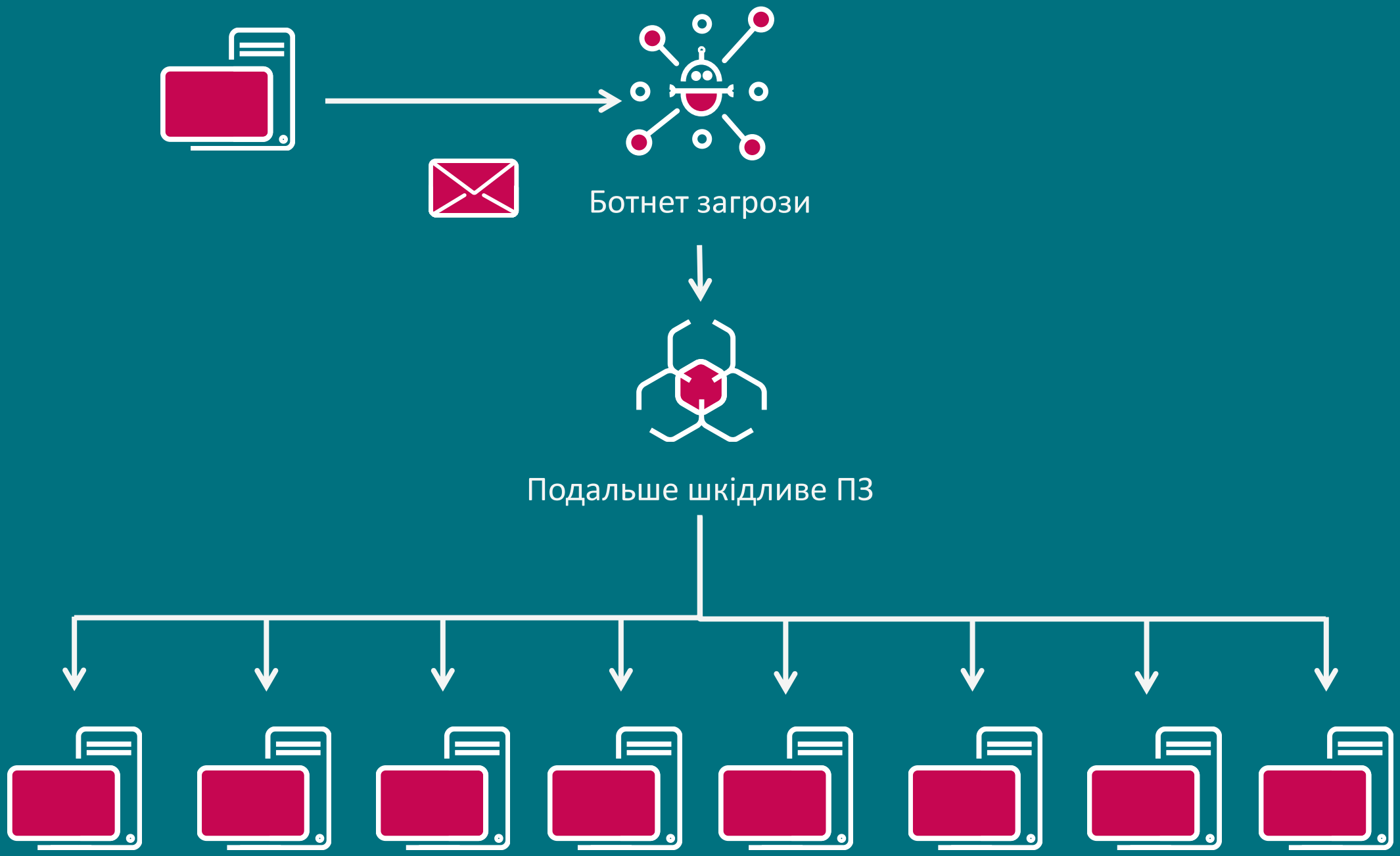
35 млрд
спроб атаки

900 000
унікальних користувачів


+768%
спроб атаки
(Q1 порівняно з Q4)
+225%
унікальних користувачів
(Q1 порівняно з Q4)
Мільйони
250
200
150
100
50
0
Тисячні
150
100
50
0
1-Jan-2020
1-Jul-2020
1-Jan-2021
RDP – спроби з’єднання (ліва вісь)
RDP – спроби з’єднання у кількості кор. (права вісь)

Фішингові кампанії


ФІШИНГ


Ботнет загрози
Подальше шкідливе ПЗ

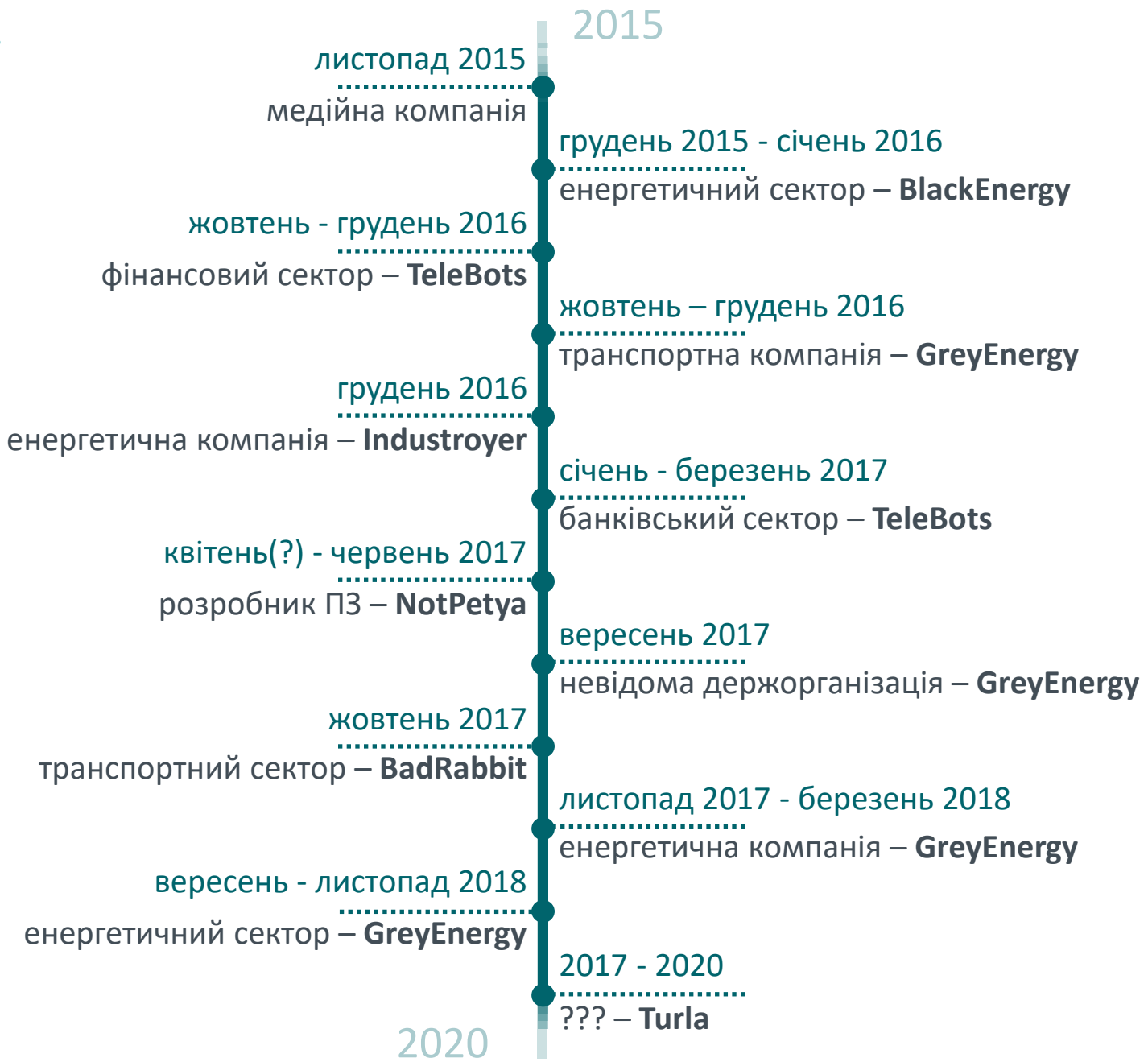
Уразливості

Відомі

Невиправлені

Найбільші кібератаки в Україні у 2015-2020

Кібератаки в Україні 2015 – 2020



ENJOY SAFER TECHNOLOGY™

Основні вектори проникнення всередину захищеної інфраструктури

Початок

Захищена інфраструктура

Фішинговий лист із зловмисним ПЗ

Носії інформації або соціальна інженерія

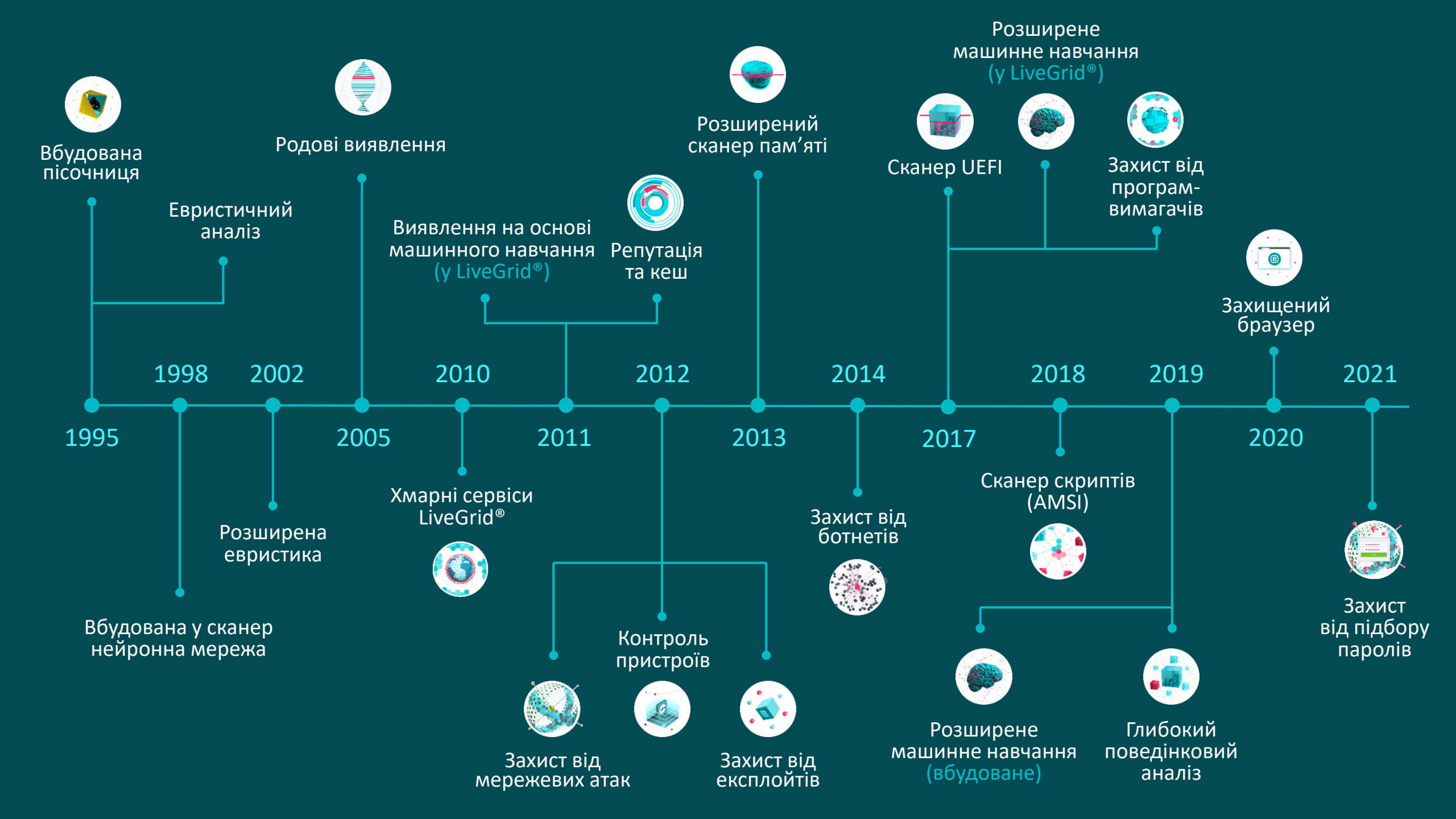
Експлуатація серверів та НЕзловмисного ПЗ

Кінець

Дані вкрадені або зашифровані

Багаторівневий захист

ТЕХНОЛОГІЇ


1995
Вбудована пісочниця
1998
Евристичний аналіз
Вбудована у сканер нейронна мережа
2002
Розширена евристика
2005
Родові виявлення
2010
Хмарні сервіси LiveGrid®
2011
Виявлення на основі машинного навчання (у LiveGrid®)
Репутація та кеш
2012
Захист від мережевих атак
Контроль пристроїв
Захист від експлойтів
2013
Розширений сканер пам’яті
2014
Захист від ботнетів
2017
Сканер UEFI
2018
Сканер скриптів (AMSI)
2019
Розширене машинне навчання (у LiveGrid®)
Захист від програм-вимагачів
Розширене машинне навчання (вбудоване)
Глибокий поведінковий аналіз
2020
Захищений браузер
2021
Захист від підбору паролів

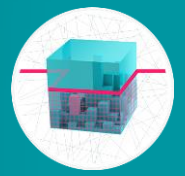
ЯДРО ВИЯВЛЕННЯ

ПЕРЕД ВИКОНАННЯМ

ВИКОНАННЯ

ПІСЛЯ ВИКОНАННЯ

Репутація та кеш



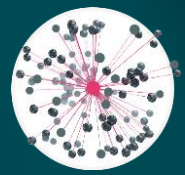
Сканер UEFI

Родові виявлення

Контроль пристроїв

Захист від програм-вимагачів

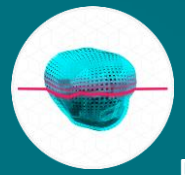
Хмарні сервіси LiveGrid®



Захист від ботнетів

Захищений браузер

Сканер скриптів (AMSI)



Розширений сканер пам’яті

Захист від експлойтів

Глибокий поведінковий аналіз

Захист від підбору паролів

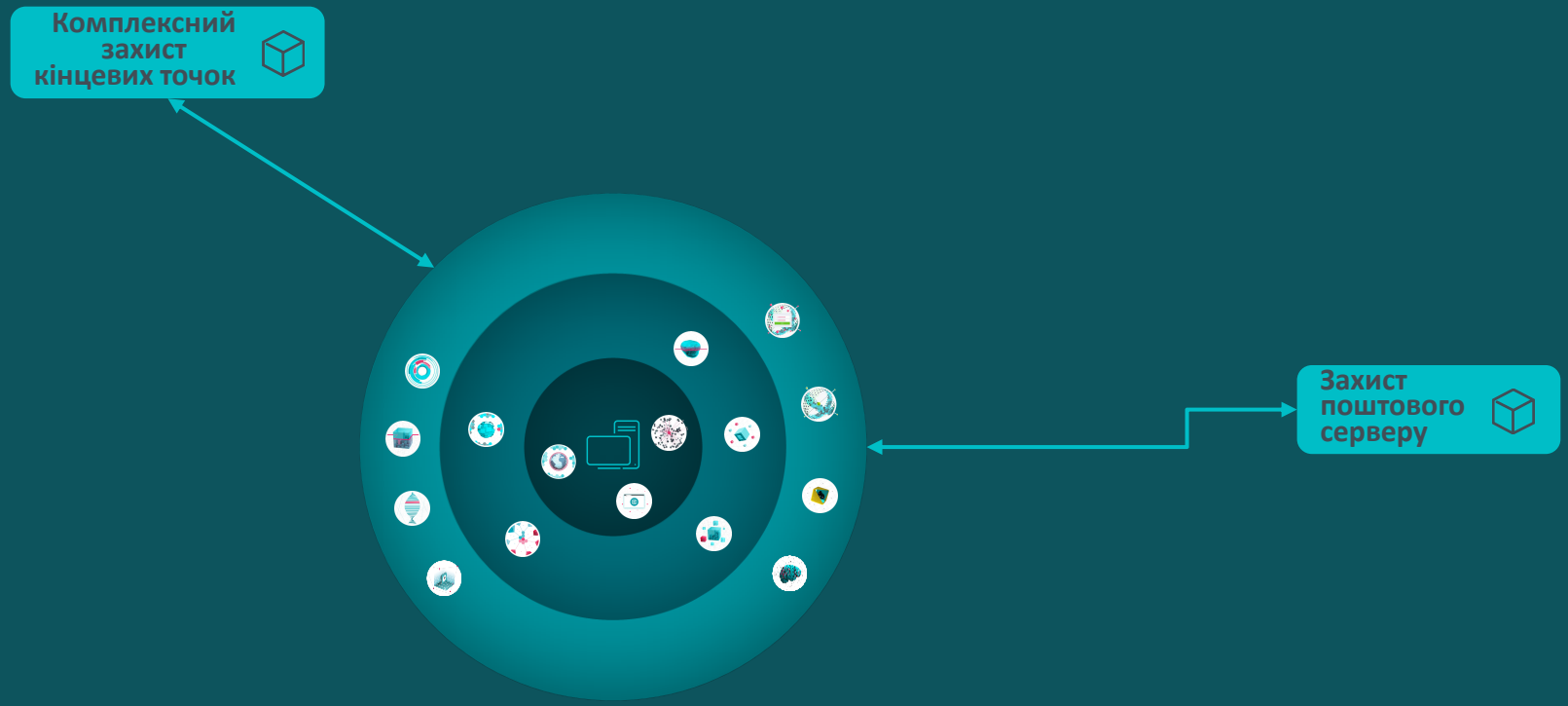
Захист від мережевих атак

Вбудована пісочниця

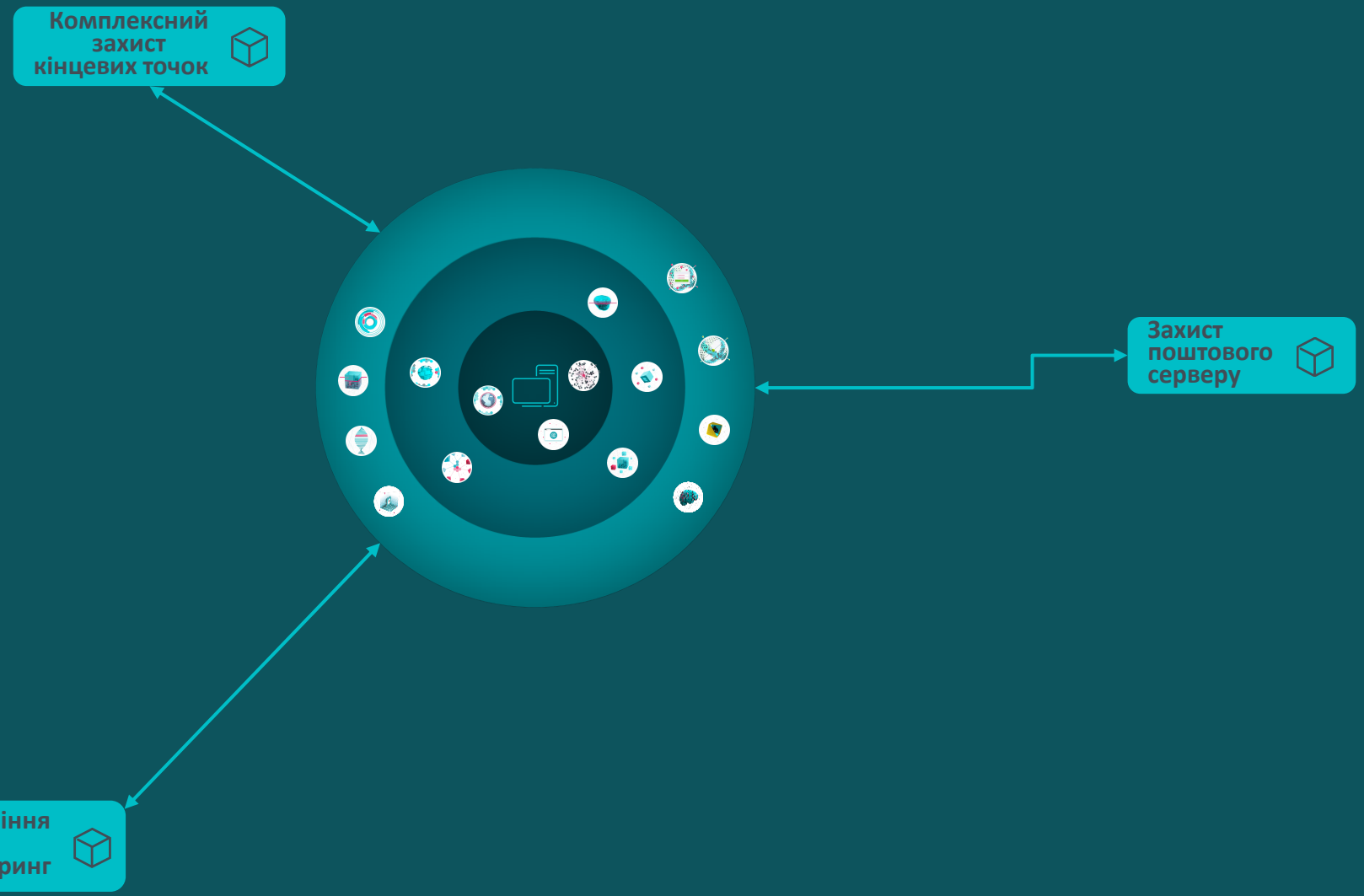
Розширене машинне навчання

ЕКОСИСТЕМА

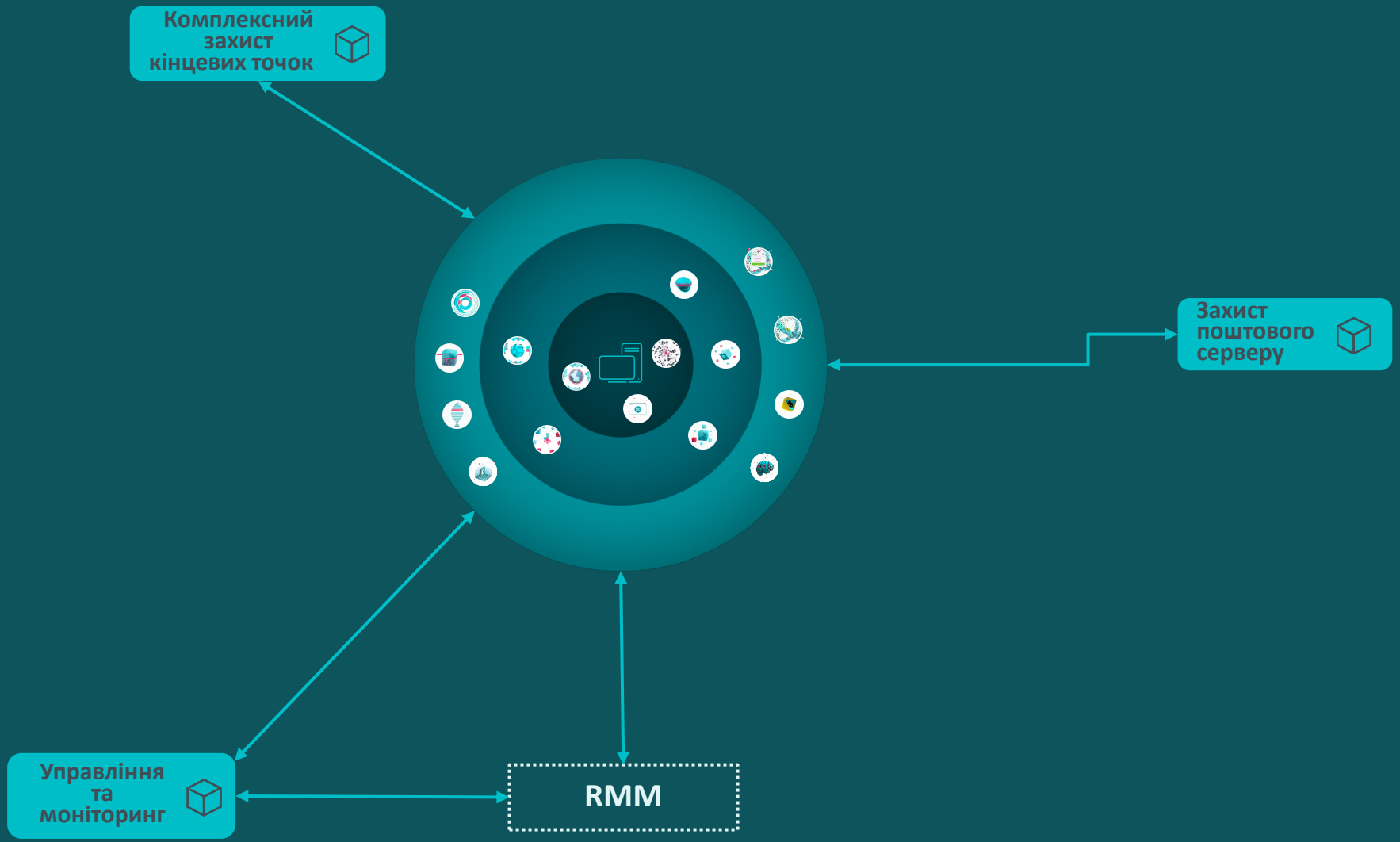
ЕКОСИСТЕМА


Комплексний захист кінцевих точок
Захист поштового серверу

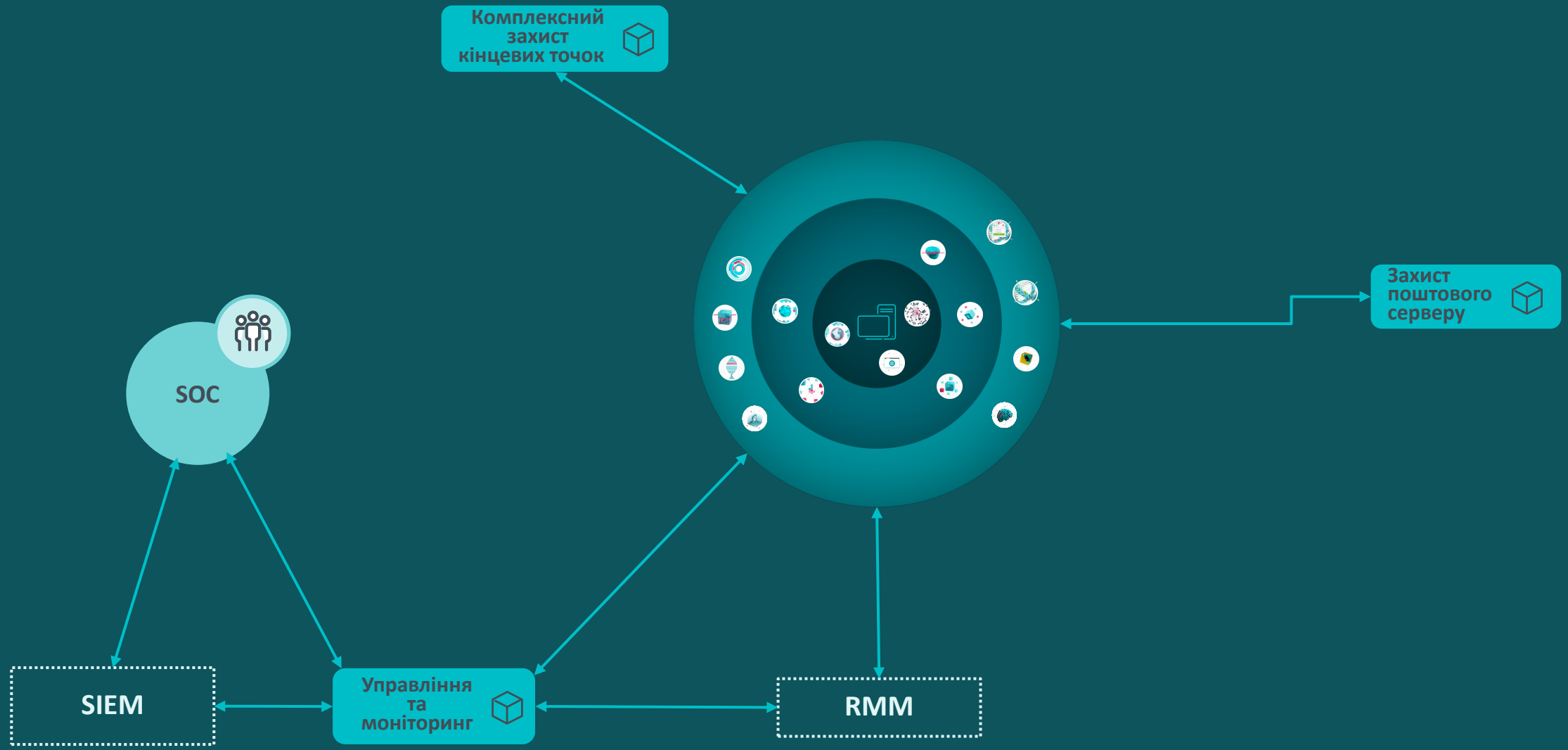
ЕКОСИСТЕМА


Комплексний захист кінцевих точок
Захист поштового серверу
Управління та моніторинг

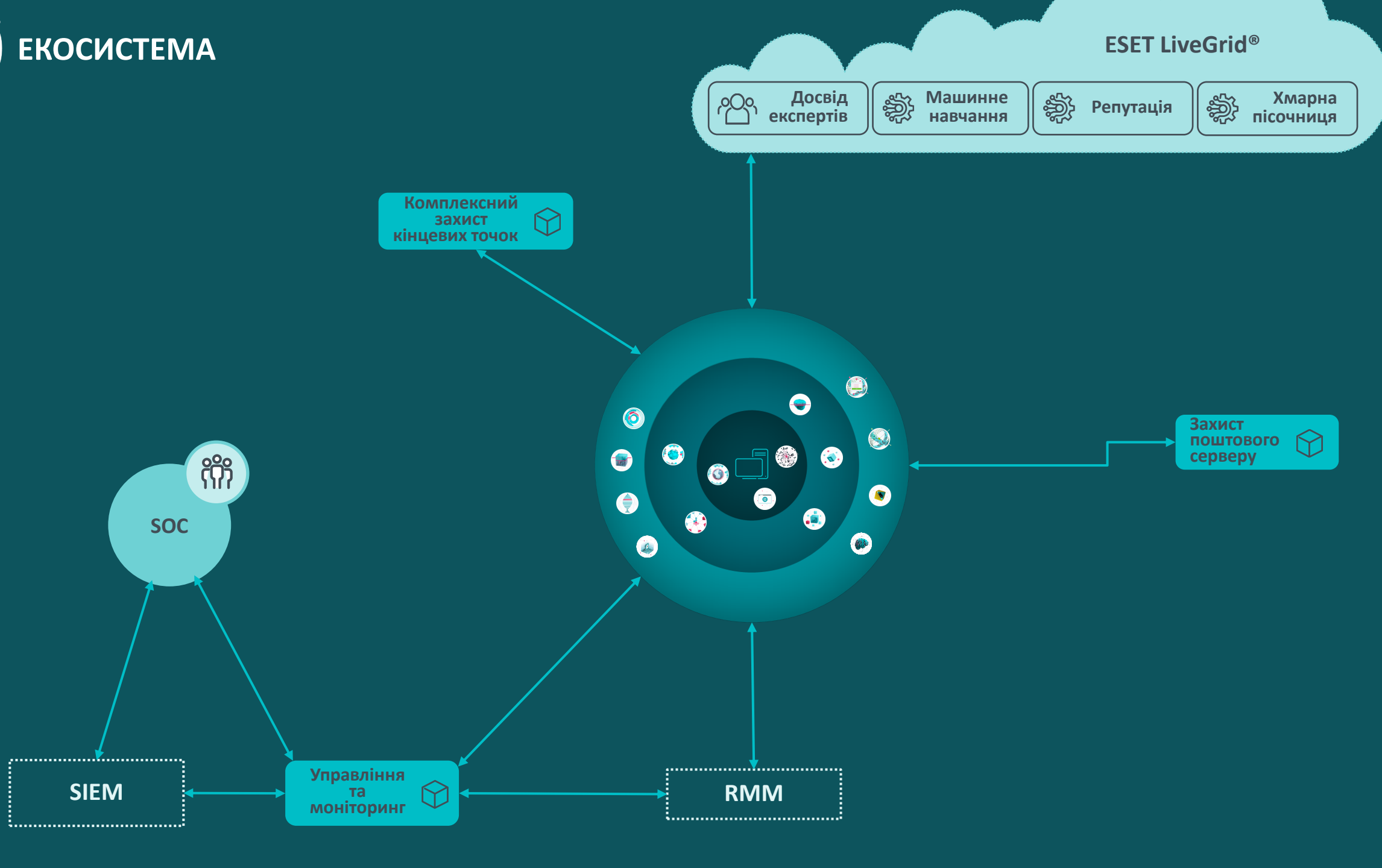
ЕКОСИСТЕМА


Комплексний захист кінцевих точок
Захист поштового серверу
Управління та моніторинг
RMM

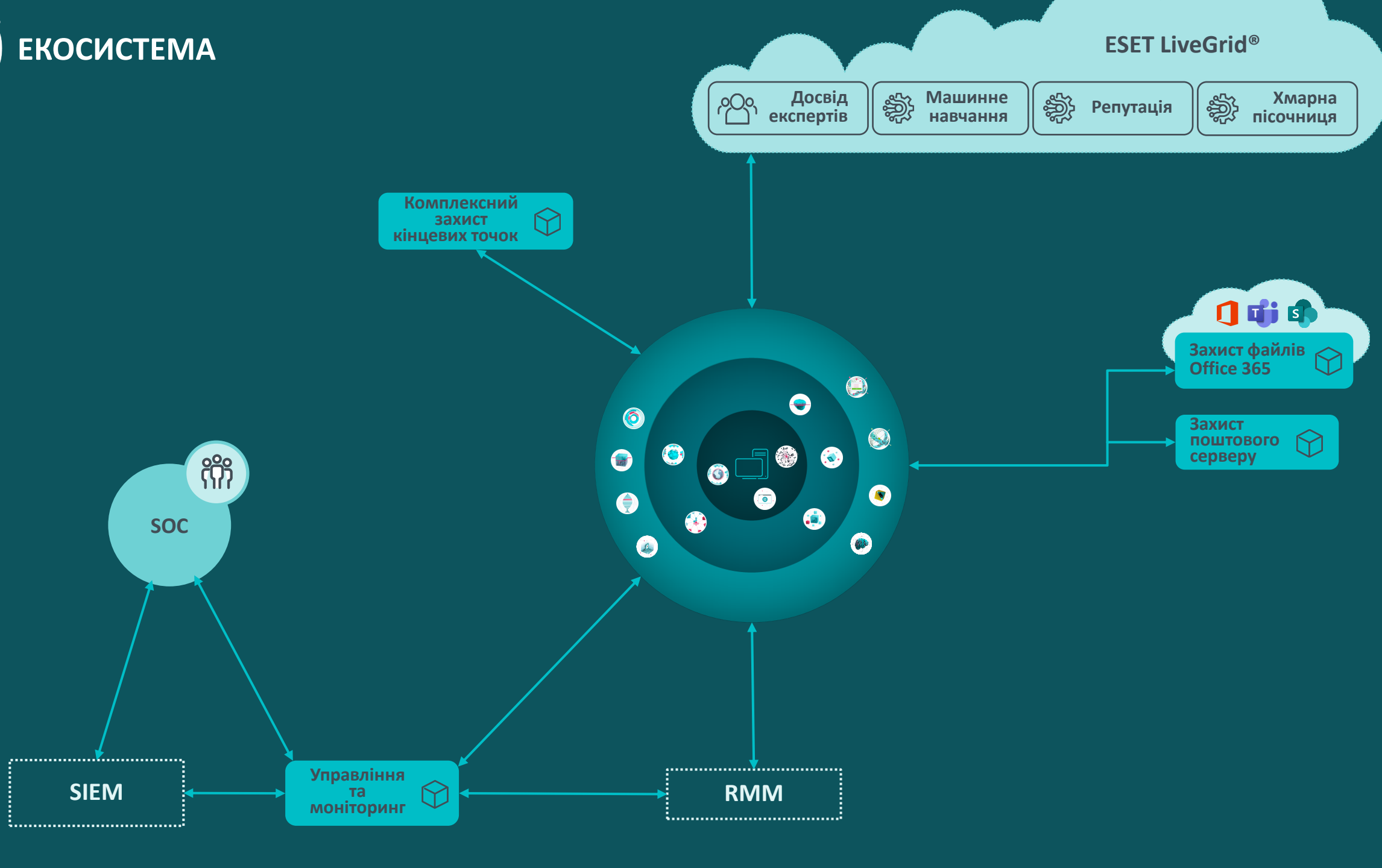
ЕКОСИСТЕМА


Комплексний захист кінцевих точок
Захист поштового серверу
SOC
SIEM
Управління та моніторинг
RMM

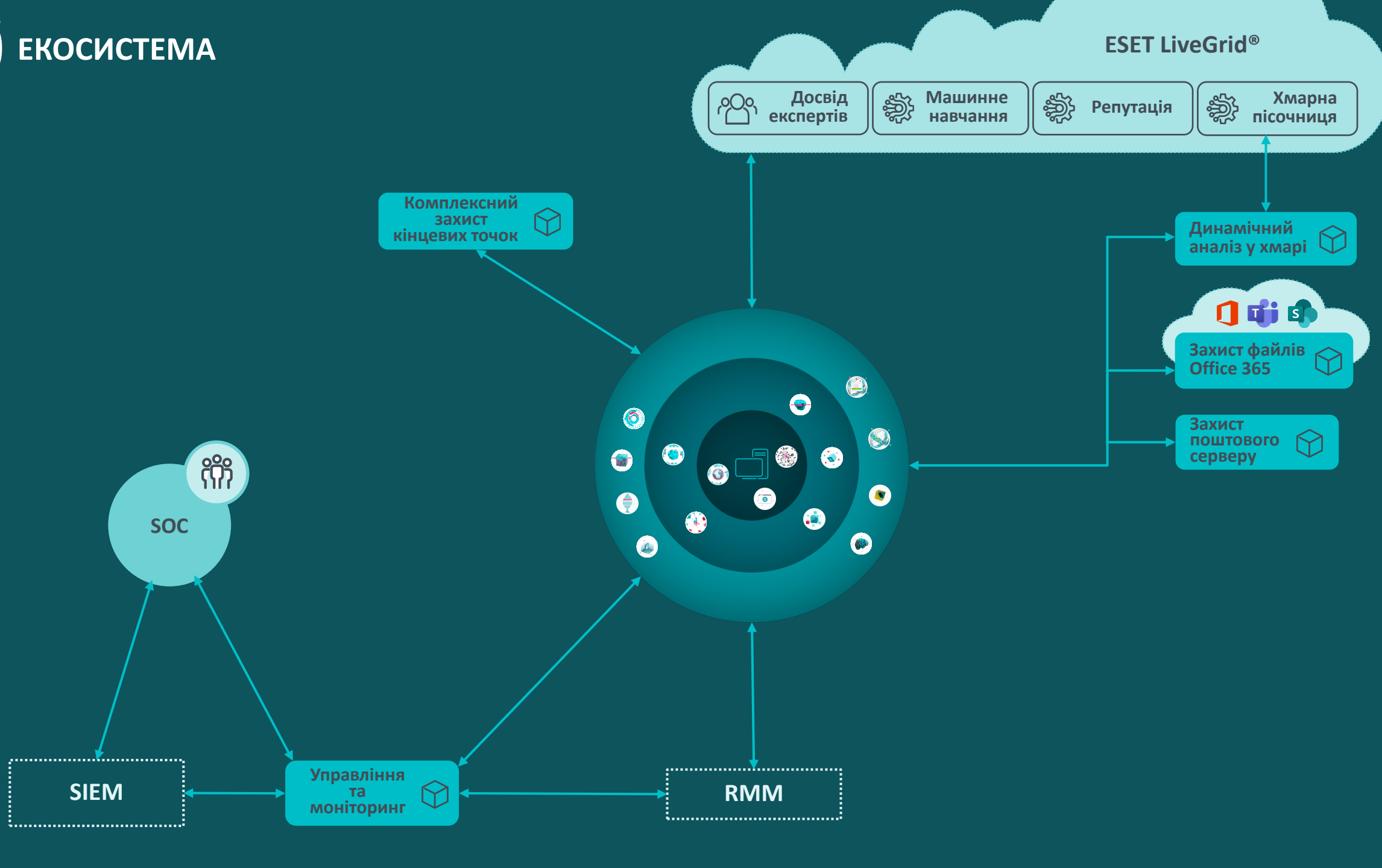
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Комплексний захист кінцевих точок
Захист поштового серверу
SOC
SIEM
Управління та моніторинг
RMM

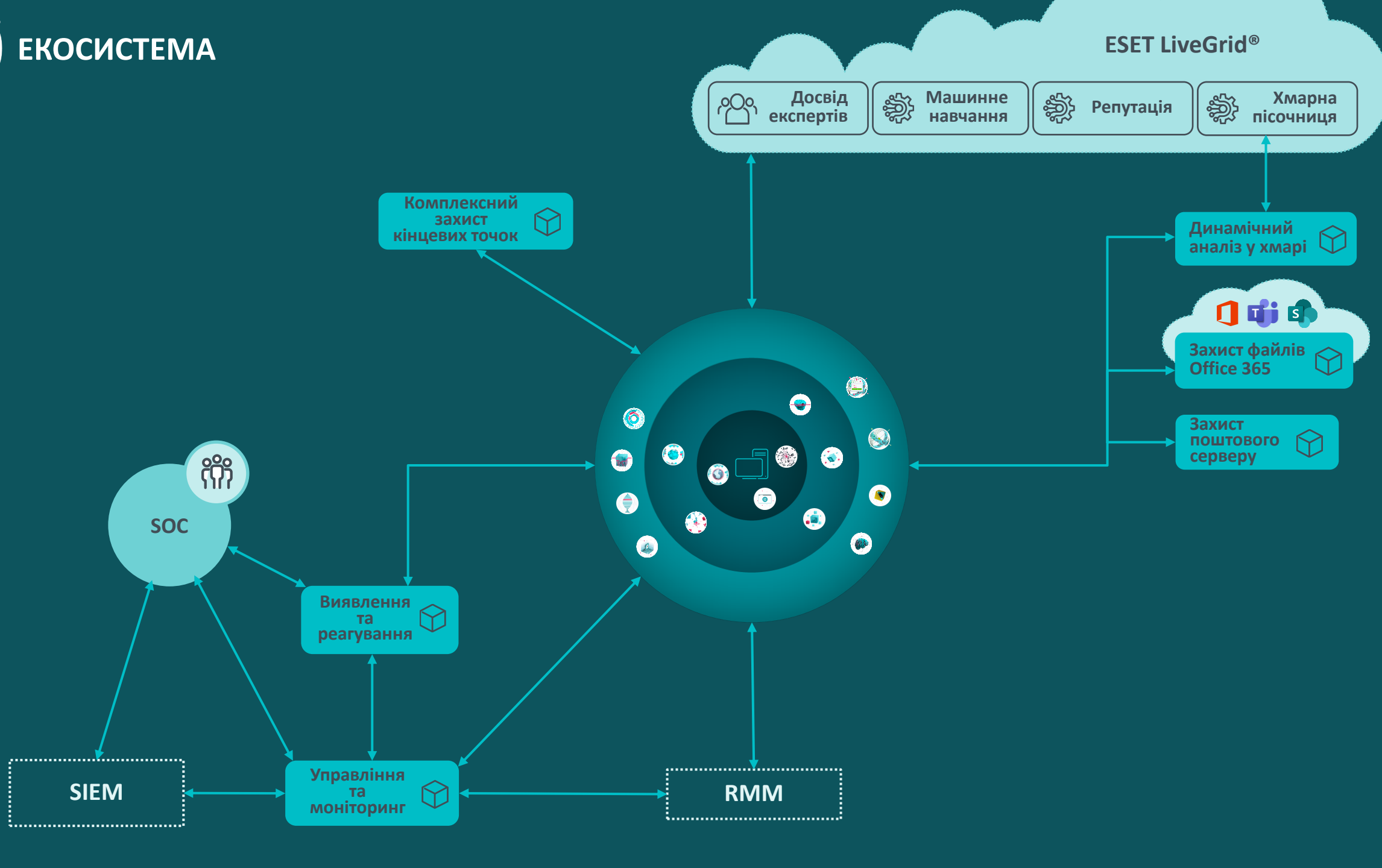
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Комплексний захист кінцевих точок
Захист файлів Office 365
Захист поштового серверу
SOC
SIEM
Управління та моніторинг
RMM

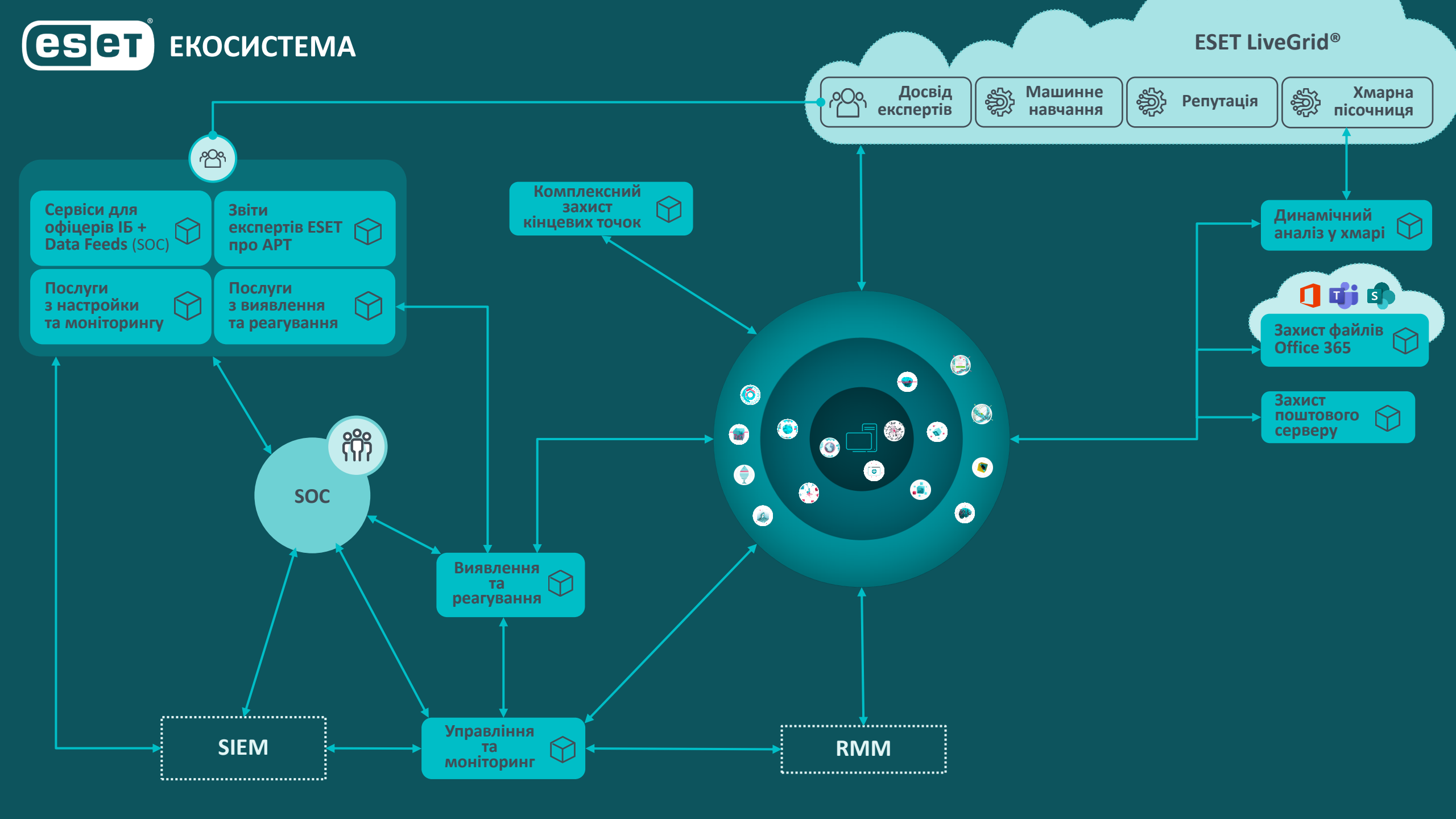
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Комплексний захист кінцевих точок
Динамічний аналіз у хмарі
Захист файлів Office 365
Захист поштового серверу
SOC
SIEM
Управління та моніторинг
RMM

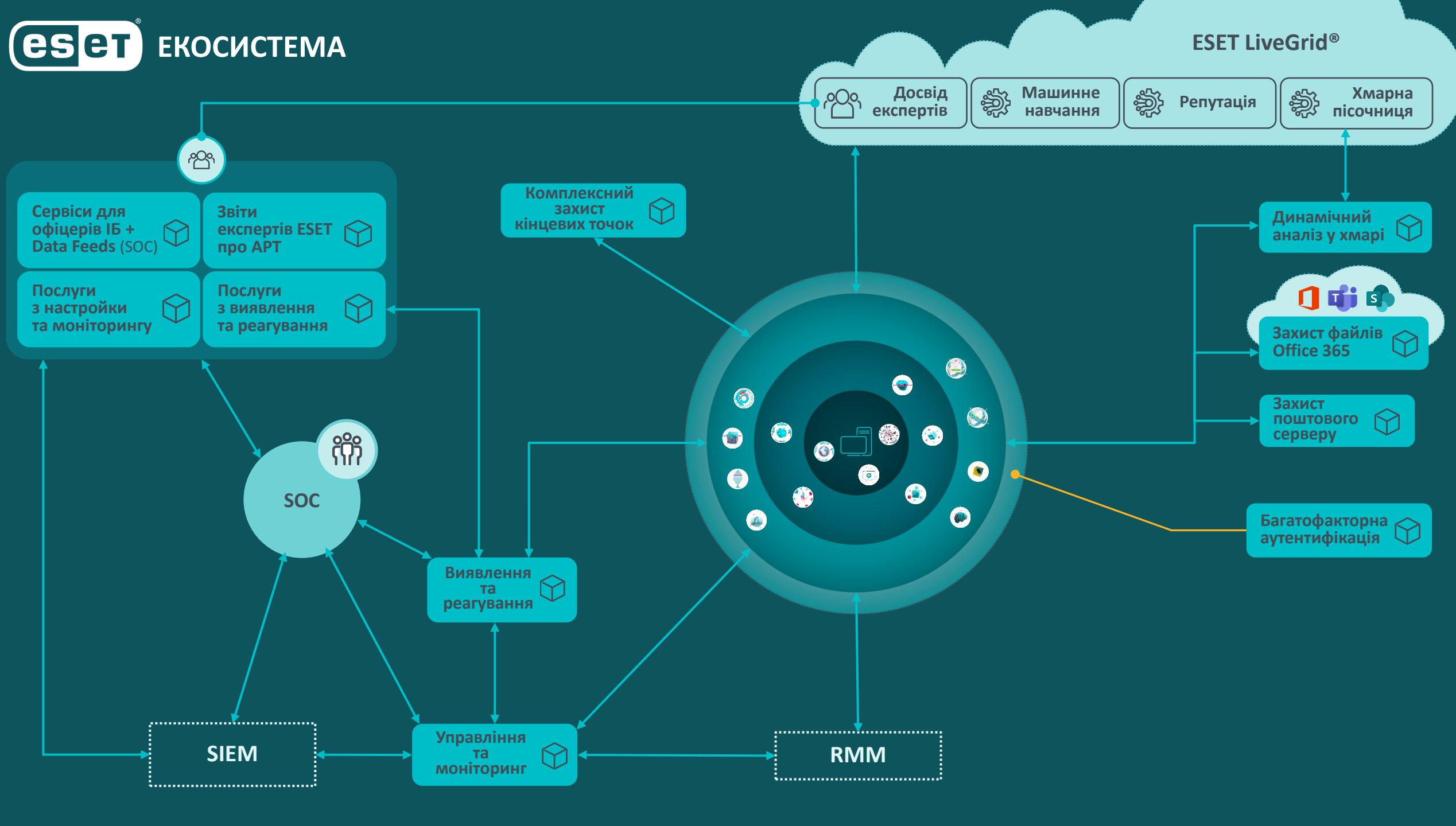
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Комплексний захист кінцевих точок
Динамічний аналіз у хмарі
Захист файлів Office 365
Захист поштового серверу
SOC
Виявлення та реагування
SIEM
Управління та моніторинг
RMM

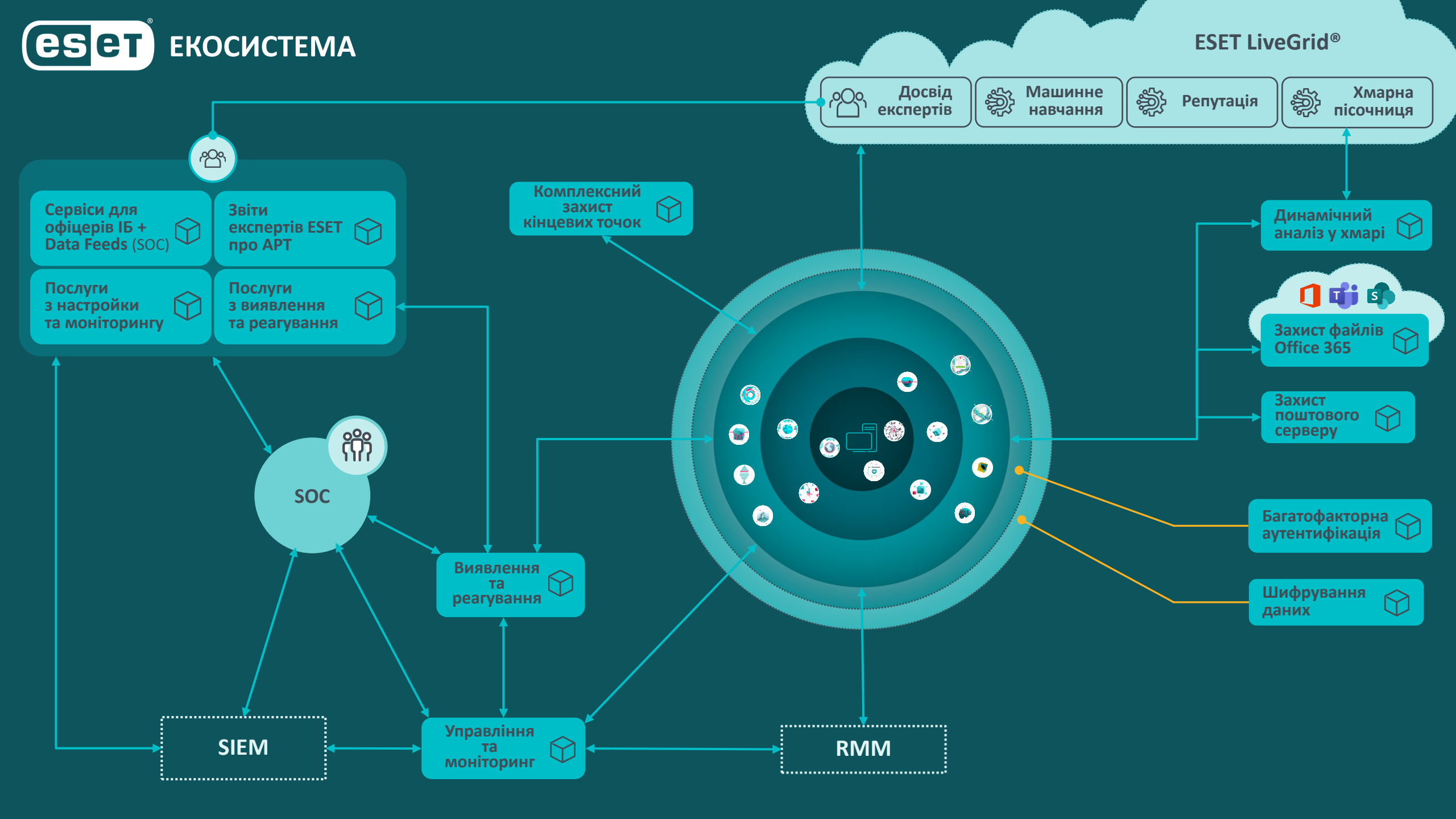
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Сервіси для офіцерів ІБ + Data Feeds (SOC)
Звіти експертів ESET про APT
Послуги з настройки та моніторингу
Послуги з виявлення та реагування
Комплексний захист кінцевих точок
Динамічний аналіз у хмарі
Захист файлів Office 365
Захист поштового серверу
SOC
Виявлення та реагування
SIEM
Управління та моніторинг
RMM

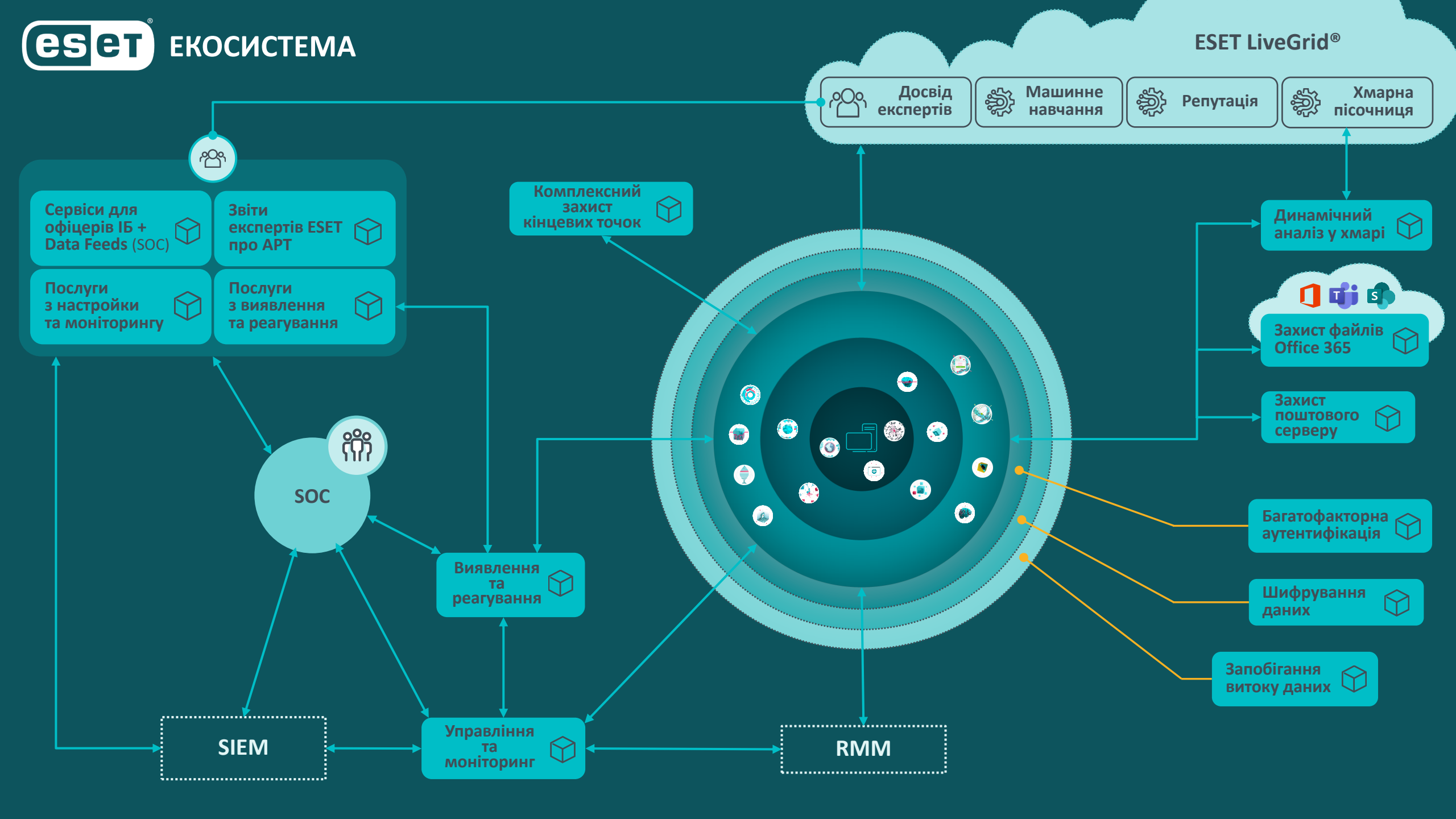
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Сервіси для офіцерів ІБ + Data Feeds (SOC)
Звіти експертів ESET про APT
Послуги з настройки та моніторингу
Послуги з виявлення та реагування
Комплексний захист кінцевих точок
Динамічний аналіз у хмарі
Захист файлів Office 365
Захист поштового серверу
Багатофакторна аутентифікація
SOC
Виявлення та реагування
Управління та моніторинг
SIEM
RMM

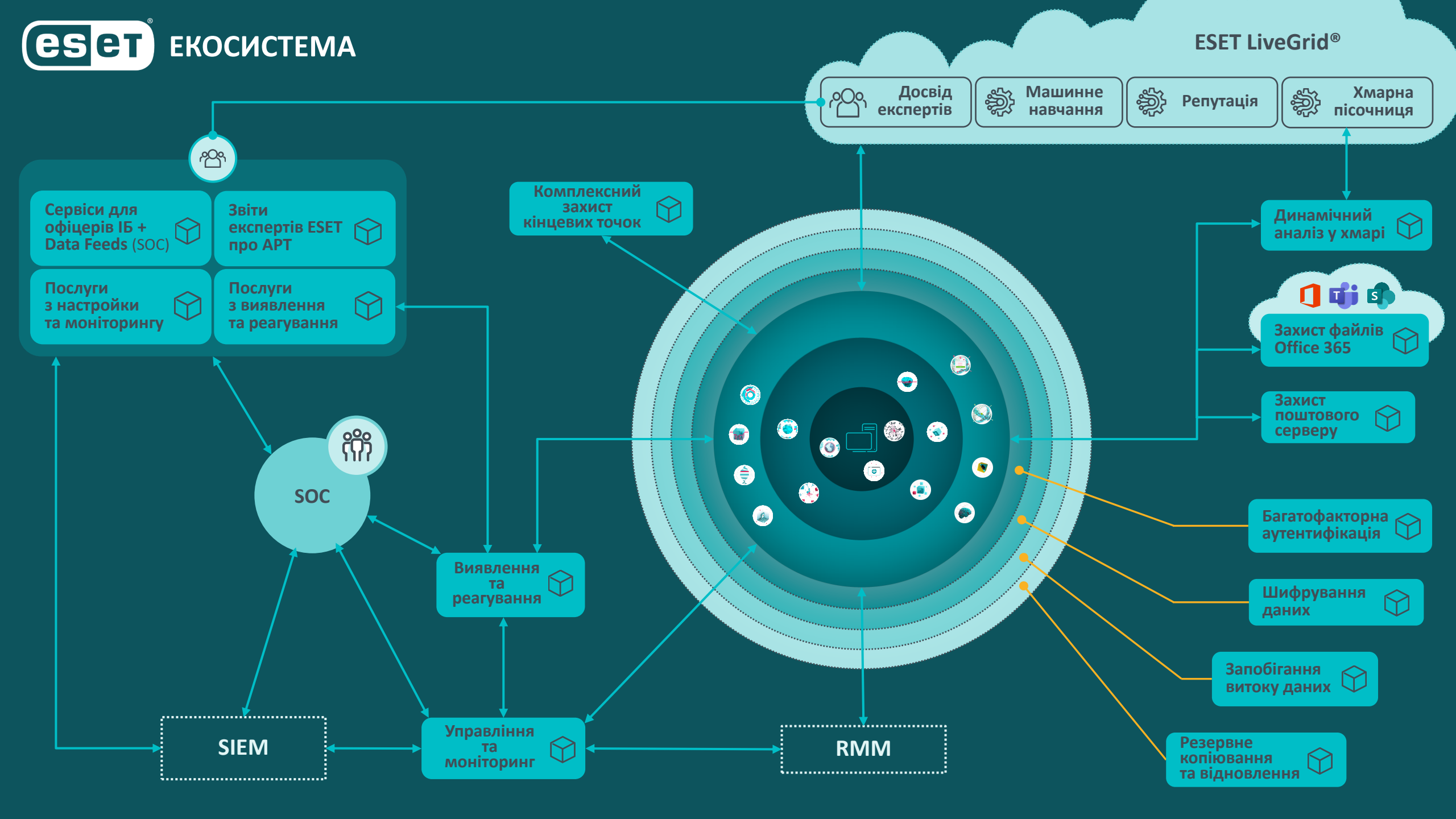
ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
Сервіси для офіцерів ІБ + Data Feeds (SOC)
Звіти експертів ESET про APT
Послуги з настройки та моніторингу
Послуги з виявлення та реагування
Комплексний захист кінцевих точок
Динамічний аналіз у хмарі
Захист файлів Office 365
Захист поштового серверу
Багатофакторна аутентифікація
Шифрування даних
SOC
Виявлення та реагування
SIEM
Управління та моніторинг
RMM

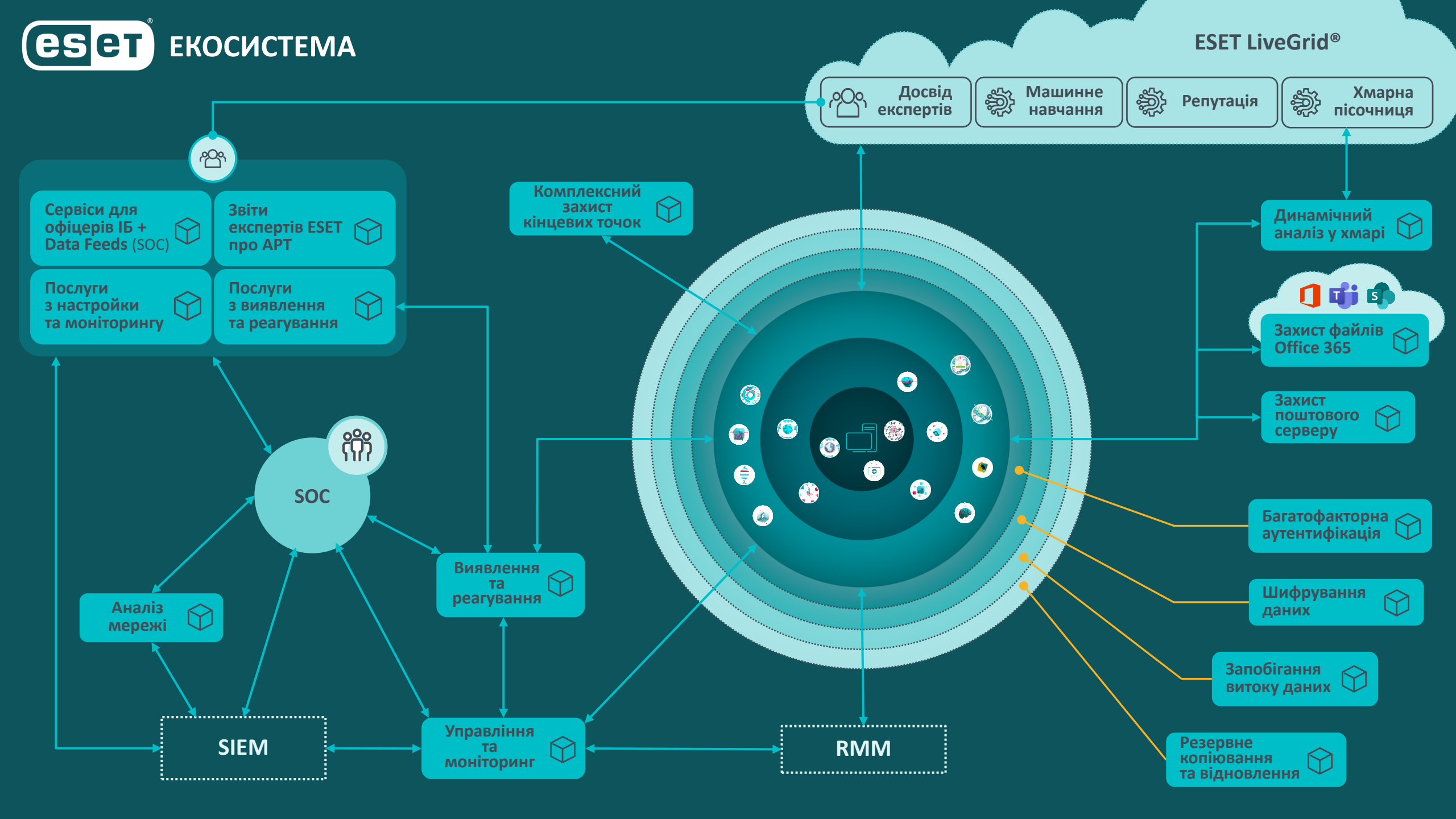
ESET ЕКОСИСТЕМА



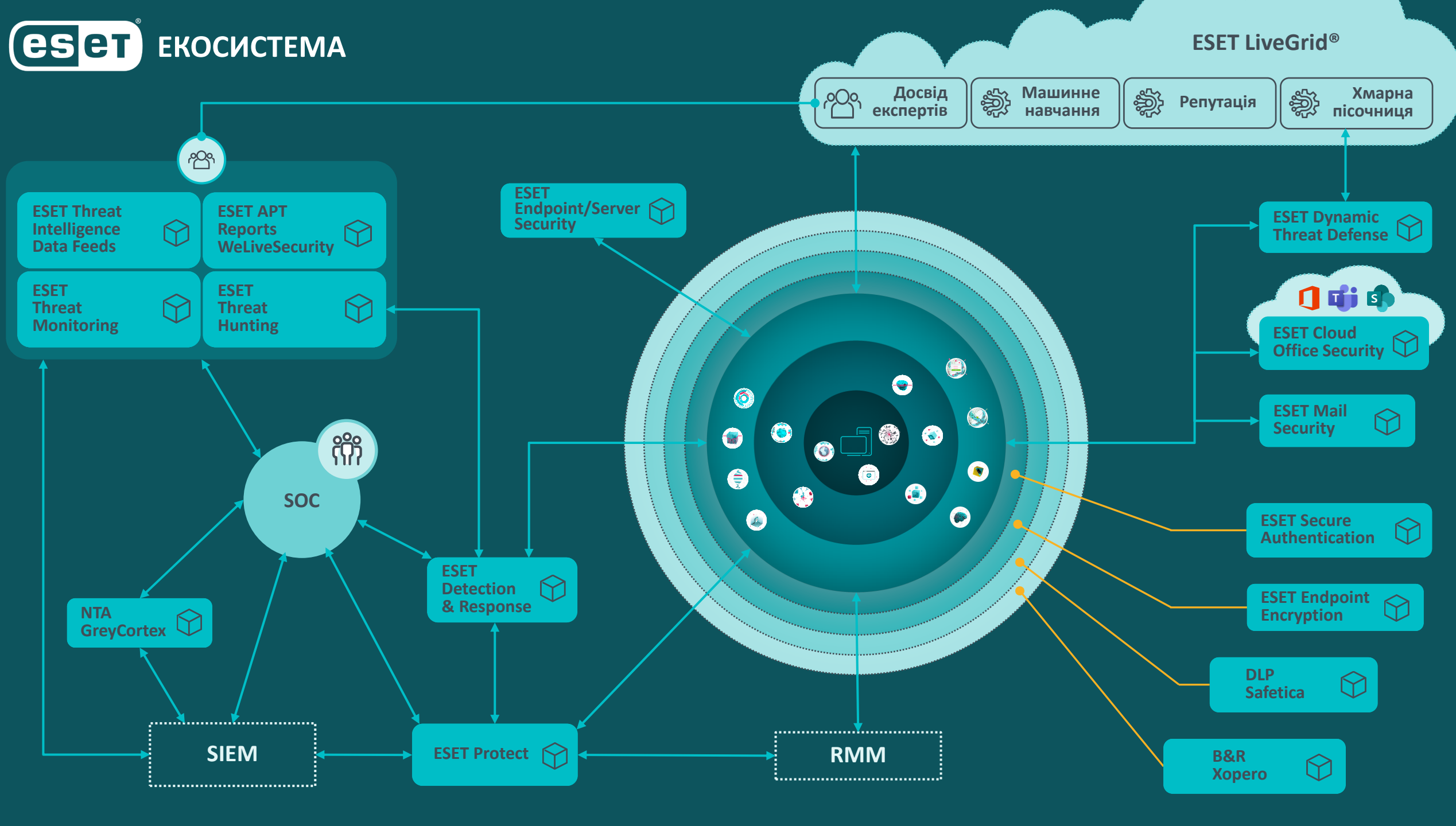
ESET ЕКОСИСТЕМА



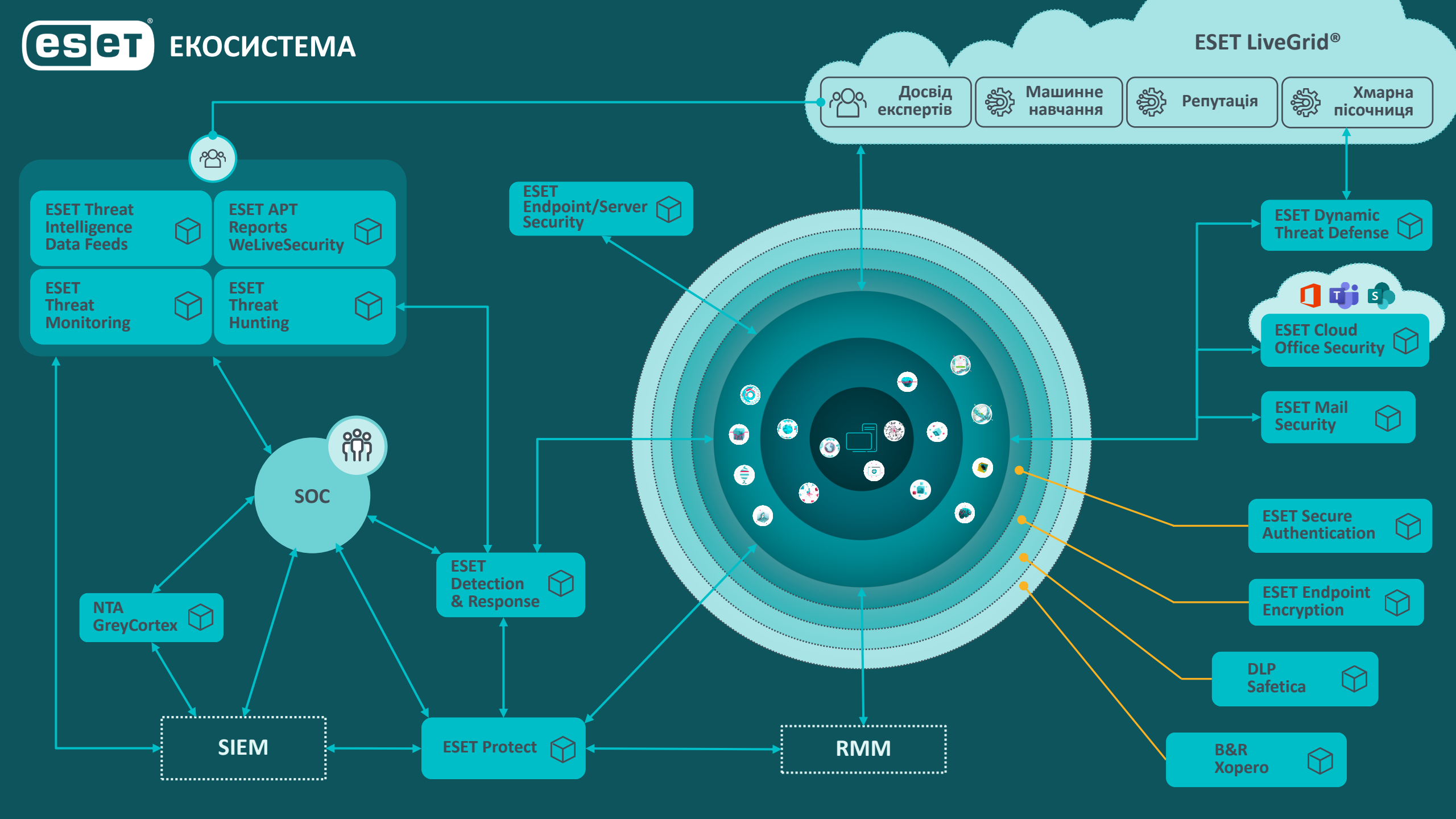
ESET ЕКОСИСТЕМА



ЕКОСИСТЕМА


ESET LiveGrid®
Досвід експертів
Машинне навчання
Репутація
Хмарна пісочниця
ESET Threat Intelligence Data Feeds
ESET APT Reports WeLiveSecurity
ESET Threat Monitoring
ESET Threat Hunting
ESET Endpoint/Server Security
ESET Dynamic Threat Defense
ESET Cloud Office Security
ESET Mail Security
SOC
ESET Detection & Response
NTA GreyCortex
ESET Secure Authentication
ESET Endpoint Encryption
DLP Safetica
B&R Xopero
SIEM
ESET Protect
RMM

ESET ЕКОСИСТЕМА



Дякую за увагу!