Cisco User Protection Suite

Ускладнюйте життя зловмисникам, а не користувачам.

Згідно з даними Talos Threat Intelligence Incident Response, 80% порушень ініціюються через націлювання на користувачів. Звідти зловмисники рухаються латерально через мережу, підвищуючи привілеї та отримуючи доступ до найбільш конфіденційних ресурсів організації.

Cisco User Protection Suite ставить користувачів у центр вашої стратегії безпеки. Захистіть всі облікові дані, пристрої та доступ до додатків для віддалених і гібридних користувачів, щоб допомогти вашій організації досягти цілей «нульової довіри» на робочому місці.

Замість того, щоб покладатися на складну мозаїку рішень безпеки, Комплексний пакет захисту користувачів Cisco зменшує складність та покращує досвід користувачів завдяки консолідованому комплексному підходу, щоб допомогти вашій організації впровадити нульову довіру без жодних перешкод.

Нульова довіра для користувачів:

Ключові інструменти User Protection Suite

Компонент пакету	Можливості
Ключові компоненти Secure Access: • Secure Internet Access • Secure Private Access	Secure Internet Access: ▪ Безпечний веб-шлюз ▪ DNS безпека Secure Private Access: ▪ Інтегрований доступ до мережі з нульовою довірою та VPNaaS Додаткові можливості включають: ▪ Моніторинг цифрового досвіду ▪ Брокер безпеки хмарного доступу (CASB) ▪ Брандмауер як послуга (FWaaS) рівня 3 та 4 ▪ Віддалена ізоляція браузера для ризикованого трафіку ▪ Secure Malware Analytics
Duo Advantage	Розширене рішення безпеки ідентифікації, що включає: ▪ Встановлення особистості (Identity Intelligence) ▪ Багатофакторна автентифікація (MFA) ▪ Безпарольна, стійка до фішингу автентифікація ▪ Єдиний обліковий запис (SSO) ▪ Автентифікація на основі оцінки ризиків ▪ Passport ▪ Довіра до пристрою та безпековий стан пристрою
Email Threat Defense	Хмарний захист електронної пошти, який розгортається за лічені хвилини та забезпечує: ▪ Повну видимість вхідних, вихідних та внутрішніх повідомлень ▪ Додатковий рівень захисту поверх шлюзу безпеки ▪ Розширене виявлення загроз на основі ШІ для точної класифікації загроз ▪ Захист від складних загроз електронної пошти, таких як компрометація ділового листування (Business Email Compromise) та захоплення облікових записів (Account Takeover) ▪ Швидку нейтралізацію інцидентів та інтеграцію з Cisco XDR

Дайте раду викликам гібридної роботи

Краща ефективність

Захист користувачів з багаторівневим захистом та інтегрованими продуктами, які краще працюють разом для захисту від еволюціонуючого ландшафту загроз.

Кращий досвід

Забезпечення гібридної роботи співробітників шляхом гарантування безперебійного та безпечного досвіду, будь-де.

Оптимізація витрат

Зменшення операційного навантаження та спрощення процесу об’єднання постачальників.

Нульова довіра для робочого місця:

До складу User Protection Suite Advantage входить User Protection Suite Essentials, плюс:

Компонент пакету	Можливості
Secure Access Advantage: ▪ Secure Internet Access ▪ Secure Private Access	Включає Secure Access Essentials (захищений доступ до інтернету та приватних ресурсів), а також: ▪ Брандмауер як сервіс (FWaaS) рівня 7 ▪ Розширену ізоляцію браузера для віддаленої роботи (Remote Browser Isolation, RBI) ▪ Запобігання витоку даних (DLP), зокрема для застосунків, що використовують генеративний ШІ
ISE Premier	ISE Premier ▪ (2 ліцензії на користувача) — захист мережі за допомогою автентифікації, авторизації та обліку доступу (AAA) ▪ Управління профілями та станом для пристроїв і користувачів, що отримують доступ до мережі ▪ Використання Secure Group Tags для уніфікації політик доступу в ISE та Secure Access ▪ Обмеження мережевого доступу для IoT-пристроїв у різних галузях, зокрема: – офіс (камери, принтери, термометри, телевізори) – лікарні (МРТ-апарати, монітори серцевого ритму) – виробництво (розумні машини) та інші
Secure Endpoint Advantage (2 пристрої на користувача)	Endpoint Threat Detection & Response включає: ▪ Антивірус та захист від шкідливого програмного забезпечення ▪ Інтегровану систему Secure Malware Analytics для блокування загроз, виявлених в екосистемі продуктів Cisco ▪ Orbital Advanced Search з аналізом шкідників для спрощення розслідувань інцидентів безпеки ▪ Захист кінцевих точок на основі ризиків із деталізованими оцінками вразливостей ▪ Інтеграцію з Cisco XDR для централізованого управління інцидентами

Об'єднайте проактивний та реактивний захист із комбінованим пакетом User and Breach Protection Combination Suite:

Базовий пакет захисту від порушень безпеки (Breach Protection Suite Essentials):
• Основний модуль розширеного виявлення та реагування (XDR Essentials)

Розширений пакет захисту від порушень безпеки (Breach Protection Suite Advantage):
• Розширений модуль розширеного виявлення та реагування (XDR Advantage)
• Розширений захист кінцевих точок преміум-рівня (Secure Endpoint Premier)
• Аналітика мережевої безпеки (Secure Network Analytics)

Преміум-пакет захисту від порушень безпеки (Breach Protection Suite Premier):
• Преміум-модуль розширеного виявлення та реагування (XDR Premier)