ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Ганченко М.І.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 9

ВСТУП ……..……. 10

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ……. 13

1.1. Призначення, структура, функції та умови функціонування системи управління привілейованим доступом в інформаційній системі організації ……... 13

1.2. Аналіз проблеми щодо управління привілейованим доступом корпоративної інформаційної системи організації……..……. 17

1.3. Мета та завдання системи управління привілейованим доступом в інформаційній системі організації…… 23

1.4. Аналіз існуючих технологій управління привілейованим доступом в інформаційній системі організації……..…. 26

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ BEYONDTRUST PRIVILEGE MANAGEMENT…..……..… 33

2.1. Призначення, можливості та функції BeyondTrust Privilege Management …….…….. 33

2.2. Компоненти та архітектура рішення BeyondTrust Privilege Management ……... 36

2.3. Призначення, архітектура рішення BeyondTrust Privileged Password та можливості щодо адміністрування…… 38

2.4. Призначення, архітектура рішення BeyondTrust Endpoint Privileged Management та можливості щодо адміністрування…… 41

2.5. Призначення, архітектура рішення BeyondTrust Secure Remote Access та можливості щодо адміністрування…… 47

2.6. Призначення, архітектура рішення BeyondTrust Cloud Security Managemen та можливості щодо адміністрування…… 52

2.7. Вимоги до системи для інсталяції рішень BeyondTrust Privilege Management……

3 РОЗРОБКА ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ BEYONDTRUST PRIVILEGE MANAGEMENT …… 54

3.1. Розробка варіанта топології та визначення критичних точок в управлінні привілейованим доступом у корпоративної інформаційної системі ……..…... 54

3.2. Технологія управління привілейованим доступом на базі рішення BeyondTrust Privilege Management для покриття визначених критичних точок у корпоративній інформаційній системі…… 62

3.3. Розробка рекомендацій щодо застосування технології управління привілейованим доступом корпоративної інформаційної системи на базі рішень BeyondTrust Privilege Management ……...……... 76

ВИСНОВКИ…….... 78

ПЕРЕЛІК ПОСИЛАНЬ..... 79

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 81

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – Персональний комп’ютер

ОС — Операційна система

ІТ — Інформаційні технології

ІБ — Інформаційна безпека

ЦОД — Центр обробки даних

PAM – Privileged Access Management

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

SNMP - Simple Network Management Protocol

SSH – Secure Shell

SSO – Single Sign-On

MFA – Multi-Factor Authentication

SAML - Security Assertion Markup Language

LSID - Life Sciences Identifier

IoT – Internet of Things

ICS -Industrial Control System

SIEM – Security Information and Event Management

IAM – Identity & Access Management

API – Application Program Interface

AD – Active Directory

GDPR – The European Union's General Data Protection Regulation

PCI DSS – Payment Card Industry Data Security Standard

HIPAA - Health Insurance Portability and Accountability Act

FDDC - Florida Developmental Disabilities Council

FISMA - Federal Information Security Modernization Act

SOX – Sarbanes-Oxley Act

NIST - National Institute of Standards and Technology

GLBA - Gramm-Leach-Bliley Act

ВСТУП

Актуальність дослідження. Корпоративна інформаційна та кібербезпека — це все про забезпечення неперервності функціонування бізнесу, шляхом використання сучасних інформаційних технологій. І з появою хмарних обчислень потреби цифрового бізнесу у сфері безпеки значно зросли, так як багатохмарні цифрові середовища вимагають багатохмарної безпеки та управління. І сьогодні, як ніколи, організаціям важливо безпечно та впевнено надавати дозволи на доступ, забезпечуючи і відстежуючи діяльність користувачів у бізнес-мережі. Адже найрозпосвсюдженішими вразливостями досі залишаються спроби отримання прав користувачів та спроби отримання прав адміністраторів. Така діяльність зловмисників, що спрямована на збої у контролях доступу призводить до неавторизованого розкриття інформації, модифікації, знищення чи використання бізнес-функцій за межами повноважень користувача та несе за собою великі репутаційні, фінансові та бізнесові втрати компаній. А оскільки, віддалена робота та хмарні послуги дедалі все більше стають рутиною, керування доступом стає базовою необхідністтю.

Privileged Access Management є найкращим рішенням для зменшення ризиків, що пов’язані з використанням привілейованих облікових записів, адміністративними доступами та правами. Оскільки PAM корпоративного рівня, що призначені для захисту, моніторингу, визначення привілейованих облікових даних і реагування на загрози, гарантують, що співробітники мають лише системні привілеї, права та дозволи, необхідні їм для виконання своєї роботи, не більше та не менше. Таким чином забезпечується найвищий рівень захисту складних розподілених середовищ – актуальних на сьогодні, а привілейований доступ отримує найвищий пріоритет у забезпеченні безпеки.

Вищенаведені аргументи актуалізують тему даної магістерської

роботи, зміст якої становлять дослідження щодо технології управління привілейованим доступом на прикладі BeyondTrust Privileged Management.

Об'єкт дослідження – процес забезпечення кібербезпеки підприємства з використанням технології управління привілейованим доступом.

Предмет дослідження – технологія управління привілейованим доступом корпоративної інформаційної системи.

Мета роботи – розробити варіант топології, визначити та покрити критичні точки в управлінні привілейованим доступом корпоративної інформаційної системи та розробити рекомендації щодо застосування даної технології на підприємстві.

Наукові завдання:

дослідити сутність проблеми управління привілейованим доступом корпоративної інформаційної системи;

встановити сутність завдань з управління привілейованим доступом;

проаналізувати існуючі технології управління привілейованим доступом;

проаналізувати методи та засоби управління привілейованим доступом;

проаналізувати основні функції та принципи реалізації управління привілейованим доступом.

розробити варіант технології, визначити критичні точки в управлінні привілейованим доступом корпоративної інформаційної системи

розробити рекомендації щодо застосування технології управління привілейованим доступом на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи управління привілейованим доступом.

Практичне значення одержаних результатів полягає в розробці варіанта топології, визначенні та покритті критичних точок в управлінні

привілейованим доступом на базі BeyondTrust Privileged Management, а також у розробці рекомендацій щодо застосування технології з управління привілейованим доступом на підприємстві.

Апробація результатів магістерської роботи було оприлюднено:

- на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ за темою “Zero Trust – однаковий рівень довіри до всього, що функціонує в межах та поза периметром компанії” [28];
- за темою “Актуальність та перспектива розвитку Privileged Access Management рішень” [29].

1. АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування системи управління привілейованим доступом в інформаційній системі організації

Управління привілейованим доступом, або ж PAM рішення, побудоване на стратегіях та технологіях кібербезпеки в IT-середовищі. Встановлюючи належний рівень управління привілейованим доступом, PAM допомагає зменшувати площу атак та запобігати збоям, пом'якшувати шкоду для організації, від зовнішніх джерел атак, а також внутрішніх, як от службова халатність, недбалість — людський фактор та інсайдери. Потенційна можливість неправомірного використання або зловживання привілеями останніх створює великий ризик безпеки для організації. Управління привілеями охоплює велику кількість стратегій, метою яких є забезпечення найменших привілеїв — обмежень прав доступу та дозволів для об'єктів, таких як: користувачі, облікові записи, програми, системи, пристрої, процеси до мінімуму, необхідного та достатнього для виконання дозволених дій.

Структурними компонентами поняття управління привілейованим доступом виступають: привілеї, привілейовані об'єкти, привілейовані облікові записи, привілейовані облікові дані, а також основний принцип найменших привілей.

У контексті інформаційних технологій привілеї розглядаються як особливе право, понаднормова перевага, повноваження, котрими наділений об'єкт для доступу до визначених ресурсів і виконання дій у межах обчислювальної системи чи мережі компанії. [1] Сам привілей відноситься до дозволу на обхід певних обмежень безпеки. [2] Привілеї для різних об'єктів вбудовані в операційні системи, файлові системи, програми, бази даних, гіпервізори, хмарні платформи

керування тощо. Залежно від перерахованих систем та їх особливостей деякі привілеї та їх делегування можуть ґрунтуватися на атрибутах, які ґрунтуються на ролях, таких як бізнес-підрозділ, а також низці інших параметрів властивих даним відділам.

Привілейованим обліковим записом являється обліковий запис у повноваженнях якого є можливість надання доступу чи привілей. Відповідно, привілейований об'єкт - це функція, користувач, програма, процес, який використовує наданий йому привілейований доступ. Привілейовані облікові записи, ще визначаються у системах як суперкористувачі, "кореневі", адміністративні та використовуються для адміністрування, надаючи практично необмежену владу у зоні власної відповідальності. Привілеї такого облікового запису мають необмежений доступ всіх видів ресурсів, включаючи файли та каталоги, із повними правами читання/запису/виконання, а також можливість відтворювати системні зміни в мережі: створення або встановлення програмного забезпечення, зміну файлів, параметрів, керування користувачами і даними. У разі використання таких високопривілейованих облікових записів, зі злим умислом, організацію очікує катастрофічна шкода. [1] Оскільки суперкористувачі вже знаходяться в межах периметру компанії. [10] Відтак найкращою практикою для будь-якої компанії є використання стандартних облікових записів користувачів для виконання своїх робочих функцій в системі, і лише IT-спеціалісти можуть мати декілька облікових записів: стандартний користувач для рутинних завдань і суперкористувач для адміністративних дій.

Так як облікові записи адміністраторів мають підвищені привілеї, вони автоматично створюють загрозу та ризик у разі неправомірного використання чи зловживання даними їм правами. І найкращим рішенням в такому випадку є наявний контроль — PAM система, що відслідковуватиме подібні облікові записи та наявні у них привілеї в рамках необхідності та визначеного часу. Прикладами привілейованих облікових записів в організації, на які може поширюватись область уваги PAM, виступають наступні:

- Локальні адміністративні облікові записи — облікові записи, які

надають адміністративний доступ лише до локальних екземплярів об’єкта. Використовуються для проведення технічного обслуговування на робочих станціях, серверах, базах даних тощо, і часто мають той самий пароль для зручності використання в усій мережі.[21]

- Облікові записи адміністратора домену — записи з привілейованим адміністративним доступом до всіх робочих станцій і серверів, що знаходяться в межах домену.[21]
- Резервні облікові записи, екстрені — записи непривілейованих користувачів, котрі матимуть адміністративний доступ до захищених систем у разі надзвичайної ситуації. З міркувань безпеки для доступу до таких облікових записів зазвичай потрібна згода керівництва, і вони зазвичай передбачають ненадійну процедуру, яка не піддається перевірці. [21]
- Облікові записи служб — привілейовані локальні або доменні облікові записи, які використовуються програмою чи службою для взаємодії з операційною системою.
- Облікові записи служби Active Directory або служб домену - мають найбільший і найнадійніший зв'язок у всій мережі, що становить загрозу безпеці, так як це повний контроль над контролерами домену та право змінювати членство кожного адміністративного облікового запису в домені. [21]
- Облікові записи програм — записи, що використовуються програмами для доступів до баз даних, виконання завдань, функцій, сценаріїв або для надання доступів іншим програмам.[1] Паролі для цих облікових записів часто вбудовані та зберігаються в незашифрованих текстових файлах, що становить загрозу безпеці.

Окрім локальних облікових записів, значного поширення набувають хмарні та віртуалізовані середовища, котрі при розширенні та модернізації використовують надмірні привілеї, доступи та дозволи. Хмари та віртуалізація окреслили поняття консолі адміністратора (наприклад, AWS і Office 365), яка надає широкий спектр можливостей суперкористувача. Крім того хмарні платформи надають і власні інструменти для управління привілейованим

доступом, що значно розширює потенціал розвитку PAM рішень та зону їх функціонування. [2]

Одними з важливих складових у функціонуванні PAM систем є поняття привілейованих облікових даних, що є підмножиною поняття облікових даних загалом. Привілейовані облікові дані пов'язані з наданням розширених доступів і дозволів для облікових записів об'єктів. Окрім того привілейовані облікові дані включають поняття привілейованих паролів та процес управління ними. Керування такими паролями має на меті безпечне зберігання, обмін, створення та обробку привілейованих паролів. Більшість компаній покладаються на готові рішення для управління привілейованим паролями для здійснення наступних завдань: відстеження та автоматизовний пошук привілейованих облікових записів та облікових даних, адаптація, контроль доступу, централізований захист, зберігання, заміна, сповіщення, звітування та нагляд за всіма обліковими даними організації які можуть надавати підвищені права привілейованого доступу. А створення та керування надійними обліковими даними є ключовою функцією у протистоянні експлойтам та кібератакам, пов'язаним зі слабкими паролями, паролями за замовчуванням, або викраденям облікових даних, що стосується порушень безпеки привілейованих облікових записів. [11]

Концепція та практики обмеження прав доступу об'єктам є необхідними у забезпеченні контролю всіх наявних та необхідних для виконання функцій доступів. У застосуванні, даний принцип визначає забезпечення мінімального рівня прав об'єкта або найнижчого рівня дозволу, маючи який об'єкт може виконувати визначену авторизовану діяльність. [1] Найменший привілей є одним із основоположних принципів моделей безпеки з нульовою довірою. Архітектури нульової довіри розглядають об'єкти як ненадійні. [2] Ефективне впровадження мінімальних привілеїв потребує політик, процедур, технологій і належної конфігурації цих технологій. Формалізація політик дозволяє краще контролювати, де зберігаються конфіденційні дані та хто може до них отримати доступ. Керування привілеями в визначеному порядку, найкращий шлях для будь-якої організації, оскільки PAM рішення завжди буде пристосоване до

унікальних потреб і ресурсів організації.

1.2. Аналіз проблеми забезпечення управління привілейованим доступом корпоративної системи організації

Необмежені привілейовані права та доступи прирівнюються до необмеженого потенціалу збитку, котрий може зазнати організація. Чим більше привілей отримує об’єкт тим більша ймовірність зловживань. Хакери, зловмисне програмне забезпечення, партнери, інсайдери, які стали шахраями, і прості помилки користувачів, особливо у випадку облікових записів суперкористувачів, є найпоширенішими привілейованими векторами загроз

Зовнішні хакери прагнуть отримати доступ та контроль над привілейованими обліковими записами і обліковими даними, знаючи, що після вони забезпечують швидкий доступ до найважливіших систем і конфіденційних даних організації. Маючи на руках привілейовані облікові дані, хакер фактично стає «інсайдером» — і це небезпечний сценарій, оскільки він може легко стерти свої сліди, щоб уникнути виявлення під час проходження скомпрометованого IT-середовища. Інсайдерські загрози розкриваються найдовше, оскільки працівники та інші інсайдери зазвичай отримують певний рівень довіри за замовчуванням, що може допомогти в уникненні виявлення. Багато з найбільш катастрофічних порушень за останні роки були здійснені інсайдерами.

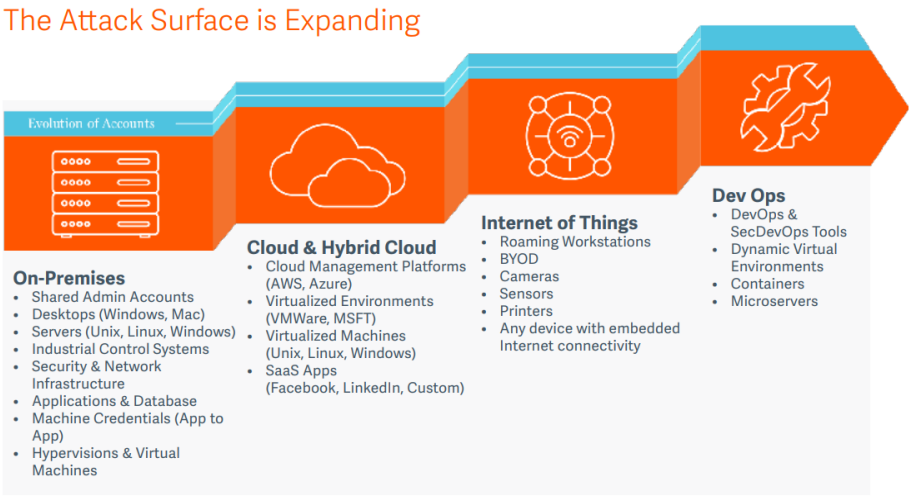

Рис. 1.1. Ускладнення завдань безпеки із розширенням традиційного периметру

Відтак, привілейовані облікові дані або ж секрети, мають передаватися безпечно, управління ними має враховувати та пом’якшувати ризики для цих секретів як під час передачі, так і у спокої. Та у міру того, як IT-екосистема стає все складнішою (див. Рис1.1), а кількість та різноманітність секретів зростає, безпечне зберігання, передача та перевірка секретів стає дедалі складнішою. [12]

І така тенденція створює ризики привілейованих облікових даних, які між іншим включають:

- Людський фактор: співробітники схильні забувати паролі через велику кількість (постійно змінних) паролів, застосовувати однакові паролі для декількох облікових записів, обирати паролі котрі легко вгадуються, записувати паролі на папері, документах, таблицях, використовувати паролі за замовчуванням. Такий підхід створює загрозу реалізації атак, таких як: зловмисники можуть використовувати автоматичні зломщики паролів, щоб вгадати паролі за замовчуванням; хакери можуть співвіднести адреси електронної пошти та імена користувачів і застосувати пароль від одного зламаного облікового запису до інших служб або облікових записів, які можуть використовувати той самий пароль, відповідно збільшуючи площу атаки.
- Ключі SSH: надмірна розповсюдженість ключів провокує наявність бекдорів для проникнення хакерів на критично важливі сервіси, а компанії не взмозі контролювати всі дійсні, неактивні та давно забуті ключі. [11]

Попередньо зазначені проблеми мають, як наслідок їх реалізації, вектор розвитку до кібератаки, метою якої є отримання незаконного доступу до підвищених прав або привілеїв, що перевищують ті, які має об’єкт — атака підвищення привілеїв. Даний тип атак поділяється на дві широкі категорії — горизонтальне підвищення привілеїв і вертикальне підвищення привілеїв. Горизонтальна ескалація привілеїв передбачає отримання прав іншого облікового запису з подібними привілеями. Як правило, це стосується облікових записів нижчого рівня - стандартного користувача, які можуть не мати належного захисту. З кожним новим скомпрометованим горизонтальним обліковим записом зловмисник розширює свою сферу доступу зі схожими привілеями. Вертикальна

ескалація привілеїв передбачає збільшення привілеїв/привілейованого доступу понад те, що вже має об'єкт. Це передбачає перехід від низького рівня привілейованого доступу до вищого рівня привілейованого доступу. [13]

Відповідно до Звіту про вразливості Microsoft за 2020 рік, опублікованого BeyondTrust, за п'ятирічний період 2015–2019 років 83% критичних уразливостей у системах Windows можна було пом'якшити, позбавивши прав адміністратора. [2] За даними Balabit, ще у 2017 році 44% витоку даних у світі відбувались з використанням привілейованих облікових даних. [4] За оцінками Forrester Research, 80% порушень безпеки стосуються привілейованих облікових даних вже у двадцятих роках 21 століття. [1] У звіті Verizon про розслідування витоку даних за 2020 рік було виявлено, що понад 80% зломів пов'язано з грубим використанням втрачених або викрадених облікових даних, а нещодавнє дослідження Centrify показало, що 74% зломів даних пов'язані з доступом до привілейованого облікового запису. [20] Незалежні дослідження, опитування та аудити показують, що постійні облікові записи з високим рівнем привілеїв поширені у фізичному, віртуальному та хмарному середовищах більшості організацій. [2] Окрім того у 2021 році проект з безпеки веб-застосунків OWASP здійснив оновлення "Top 10 Web Application Security Risks" [3] вразливостей і вразливість "Broken Access Control було піднято з п'ятої позиції" на першу (див. Рис.1.2) та зазначено, що 94% додатків було перевірено на певну форму, включаючи можливість підвищення рівня привілей і діяльність від імені адміністратора, зламаного контролю доступу.

Рис. 1.2. Top 10 Web Application Security Risks

Як повідомляється в щорічному звіті IBM Security X-Force Insider Threat Report [5] за 2021 рік 40% інцидентів стосується співробітників з привілейованими правами доступу до активів компанії, і у 100% інцидентів з поданих 40%, коли інсайдер був підтверджений або ж мав адміністративний доступ, де останній і зіграв свою роль у цьому інциденті. І лише в Україні на кінець 2021 року системою виявлення вразливостей і реагування на кіберінциденти на об'єктах моніторингу зафіксовано підозрілі події, де перші місця посідають інциденти з порушення прав адміністраторів – 22% від загальної кількості [6], а отже спроб отримання привілейованого доступу.

На жаль, використання облікових даних в реалізації атак підвищених привілеїв стосується всіх організацій, незалежно від того, в якій з операційних систем (див. Рис.1.3) вони створюють привілейовані облікові записи та зберігають привілейовані облікові дані.

Operating System	Credential Exploitation	Vulnerabilities & Exploits	Misconfigurations	Malware	Social Engineering
Windows	H	H	M	H	H
macOS	H	M	L	M	H
Unix	H	M	M	L	L
Linux	H	H	H	M	H
Infrastructure	H	M	M	L	L
IoT	H	M	H	L	L
IoT	H	L	H	L	L

Рис. 1.3. Ймовірність реалізації атак в ОС (H – висока частота та ймовірність вектора атаки з широким спектром загроз для організації; M – середня ймовірність вектора атаки на організацію з середніми шансами на широкомасштабний успіх; L – рідкісна або нечаста атака на організацію та низька ймовірність того, що вона буде успішною)

Деякі операційні системи більш схильні до соціальної інженерії просто на основі взаємодії користувача. Наприклад, соціальна інженерія є більш

поширеним фактором атак на підвищення привілеїв Windows. З іншого боку, атаки на підвищення привілеїв на Unix і Linux рідко є результатом соціальної інженерії, а скоріше є результатом неправильної конфігурації, уразливостей і експлойтів, а також цілеспрямованих інсайдерських атак. Використовуючи такі технології, як SSO і MFA, організації можуть зменшити ризик, та поєднуючи такі підходи з системами управління привілейованим доступом з'являється більш потужний захист.[13]

Хоча принцип найменших привілей котрий використовують PAM системи є доволі простим, та і він зазнає деяких складнощів у реалізації, при наявності варіативних змінних, таких як: гетерогенні системи (Windows, macOS, Unix, Linux тощо), різнотипні програми та надмірність кінцевих точок (настільні комп'ютери, сервери, ноутбуки, планшети, смартфони, IoT, ICS тощо), різноманітність обчислювальних середовищ (хмарні, віртуальні, локальні, гібридні), різнотипність ідентифікаторів та ролей користувачів, доступність розробників та постачальників. Тож Компанії у спробах запровадити політики і технологічні рішення для реалізації найменших привілей, зіштовхуються з численними факторами, котрі перешкоджають встановленню оптимальної кількості прав та привілей, доступів. Такими факторами є:

- відсутність поінформованості про всі наявні привілейовані облікові записи, активи та облікові дані в масштабах організації;
- різноманіття систем та програм, що мають облікові дані за змовчуванням, що є легко вгадуваними;
- неналежне налаштуванням та керування додатками та системами;
- опір працівників щодо обмежень доступів, котрі порушують процеси користувача, перешкоджаючи продуктивності;
- широкий набір привілеїв у кінцевих користувачів, для уникнення надлишкових запитів до служб підтримки;
- накопичення нових обов'язків та збереження старих привілей чи відсутність відношення їх до встановленої ролі;
- відсутність контекстної деталізації, для надання доступів лише за

необхідності та для конкретного використання;

- давно забуті привілейовані облікові записи, що розкидані в організації;
- спільність облікових записів та паролів у розпорядженні IT-команди, яка використовує велику кількість привілейованих облікових даних для зручності розподілу обов'язків та робочих навантажень;
- повторюваність у використанні одних і тих же облікових даних для декількох облікових записів;
- непослідовність адміністрування платформ та середовищ.[2]

Деякі з сучасних загроз від IoT, DevOps і хмарних середовищ є новим джерелами ризиків та проблем, що пов'язані з привілейованим доступом, і включають:

- Консолі та середовища адміністратора хмари та віртуалізації. За допомогою цих консолей користувачі можуть без особливих зусиль запускати тисячі віртуальних машин і керувати ними. Організаціям потрібні правильні привілейовані засоби контролю безпеки, щоб інтегрувати та керувати всіма цими новоствореними привілейованими обліковими записами й обліковими даними у великих масштабах.
- Середовища DevOps. Акцент DevOps на швидкості, хмарних розгортаннях і автоматизації створює багато викликів і ризиків для управління привілеями. Організаціям часто бракує уявлення про привілеї та інші ризики, створені контейнерами та іншими новими інструментами. Неадекватне керування секретами, вбудовані паролі та надання надмірних привілеїв – це лише деякі ризики, пов'язані з пов'язаними привілеями в типових розгортаннях DevOps.
- Пристрої Edge Computing & IoT. Доступ до цих пристроїв і з них, а також самі пристрої мають бути захищені. Ця проблема ускладнюється тим, що пристрої IoT зазвичай мають серйозні недоліки безпеки, такі як жорстко закодовані паролі за замовчуванням і неможливість посилити програмне забезпечення або оновити мікропрограму.

Ще одним аспектом виникнення ризиків для організацій є доступи постачальників. Типові методології, які використовуються для доступу постачальників, визначають те, що організації повинні жити в умовах відсутності видимості та детального контролю над цими доступами. Іноді постачальники використовують такі технології, як VPN, які забезпечують повний тунель через мережу компанії для доступу до її активів, що не дає жодних гарантій того, що постачальники не запровадять шкідливе програмне забезпечення в організаційне середовище, не використовуватимуть свій доступ неналежним чином або не допускатимуть помилок, які зможуть створити надмірний ризик. Облікові дані постачальників можуть бути слабкими, доступ може бути спільний між постачальниками та їхніми співробітниками, а паролі можуть використовуватися повторно та/або бути застарілими. Усі ці ризики посилюються, коли користувач має привілейований доступ до середовища компанії для виконання функцій постачальника чи підрядника. Відтак, вимірюючи даний ризик постачальник може бути найслабшою ланкою у безпеці всього підприємства. Тож керування привілейованим доступом постачальника - це забезпечення безпечного та безперебійного доступу, а також пом’якшення ризиків шляхом поширення передових практик керування привілейованим доступом за межами периметра організації. [14]

1.3. Мета та завдання системи управління привілейованим доступом в інформаційній системі організації

PAM складається зі стратегій і технологій кібербезпеки для здійснення контролю над підвищеним доступом (локальним або віддаленим) і дозволами для ідентифікаторів, користувачів, облікових записів, процесів і систем у середовищі — на місці або в хмарі. [14] Захист від несанкціонованого доступу є найактуальнішим питанням у кіберзахисті, оскільки хакери постійно намагаються отримати доступ до облікових записів, щоб використати їх для наступних атак. [6] І безпека привілейованого доступу є вкрай важливою,

оскільки вона є базою для всіх інших гарантій безпеки, так як має: [8]

- великий вплив на бізнес, а відповідно втрати репутації, даних;
- високу ймовірність ураження через виникнення, розповсюдження нових методів та вразливостей.

Впровадження керування привілеями не лише мінімізує ймовірність порушення безпеки, але й допомагає обмежити обсяг порушення. Впровадження найкращих практик PAM також є важливою частиною зміцнення IT-систем підприємства. Gartner визначає впровадження PAM – пріоритетом номер один в проектах безпеки на найближчі роки. [4] Адже своєчасне впровадження PAM системи дозволяє вберегтись від можливих інсайдерських атак зі сторони адміністраторів і вищого керівництва компаній, а також контролювати діяльність аутсорсингових компаній і забезпечити відповідність вимогам законів і стандартів у сфері ІБ.

Рішення PAM надають основні переваги, зокрема:

- Конденсована поверхня атак - обмеження привілеїв для людей, процесів і програм означає, що шляхи та входи для експлойтів також зменшуються.
- Зменшення зараження та розповсюдження зловмисного ПЗ. Усунення надмірних привілеїв, шляхом застосування мінімальних привілеїв у всій організації, може запобігти закріпленню зловмисного програмного забезпечення або зменшити його поширення.
- Покращена операційна продуктивність - обмеження привілеїв мінімальним діапазоном процесів для виконання авторизованої діяльності зменшує ймовірність проблем несумісності між програмами чи системами та допомагає знизити ризик простою.
- Централізоване управління привілейованим доступом та моніторинг життєвого циклу кожного наданого привілейованого права.
- Контроль якості — управління групами найбільшого ризику — підрядниками, та збереження якості даних у сховищах облікових записів.
- Дотримання політики безпеки компанії — виявлення ризиків, що пов’язані з політиками використання PAM рішень та передбачення їх впливу на бізнес-

процеси організації.

- Досягнення та підтвердження відповідності. Привілейоване керування доступом допомагає створити менш складне, а отже, більш зручне для аудиту середовище. В свою чергу аудит PAM систем надає можливість переконатись, що компанія дотримується найкращих методів використання PAM. [22]

Одна з головних цілей керування привілеями — це допомога організаціям краще відповідати вимогам відповідності Sarbanes-Oxley, ISO 27001, PCI DSS тощо. [22] Крім того, багато нормативних актів, зокрема HIPAA, PCI DSS, FDDC, Government Connect, FISMA та SOX вимагають від організацій застосовувати політики найменшого доступу для забезпечення належного управління даними та безпеки систем. [1] Мандат федерального уряду США FDCC передбачає, що федеральні службовці повинні входити в ПК зі стандартними привілеями користувача. Правило конфіденційності HIPAA надає вказівки щодо встановлення найменших привілеїв, наприклад обмеження доступу до даних на основі «мінімально необхідного використання» для досягнення цілей. PCI DSS стверджує, що організації, які обробляють або зберігають дані кредитних карток, повинні обмежувати доступ до даних власників карток за діловими потребами, і зокрема вимагає використання облікових записів користувачів з найменшими привілеями. [2] Багато фреймворків NIST, у тому числі для реалізації принципів нульової довіри (архітектури нульової довіри та доступ до мережі з нульовою довірою), також підкреслюють необхідність PAM. Можливості моніторингу та управління привілейованим сеансом також є важливими для відповідності. SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA та інші нормативні акти вимагають від організацій не лише безпеки та захисту даних, але й здатності довести ефективність цих заходів. [1]

Саме тому PAM рішення корпоративного рівня призначені для захисту, моніторингу, визначення привілейованих облікових даних і реагування на загрози. PAM надає детальну видимість, контроль і аудит над привілейованими ідентифікаторами та діями. [1] Цей додатковий рівень безпеки захищає критично важливі бізнес-системи, а також сприяє кращому управлінню та дотриманню

норм щодо даних. [20]

Збільшення площ атак, підвищені ризики безпеки, необхідність рухатись у ногу з сучасними робочими бізнес-процесами – усе це вимагає впровадження нових рішень PAM із підвищеним рівнем безпеки, автоматизацією, а також інтеграцією у хмарне середовище. Таким чином відбувається максимальних захист складних розподілених середовищ. [9] І так як перехід на віддалену роботу додатково зменшує простір для контролю [8] – PAM стає вирішенням для подібних проблем.

1.4. Аналіз існуючих технологій управління привілейованим доступом в інформаційній системі організації

У 2020 році у The Cost of Insider Threats: Global Report [15] зазначається, що лише 39% огранізацій прийняли ту чи іншу форму PAM А станом на лютий 2022 року лише 27% компаній країн СНД використовують PAM-системи (Рис.1.4). [16]

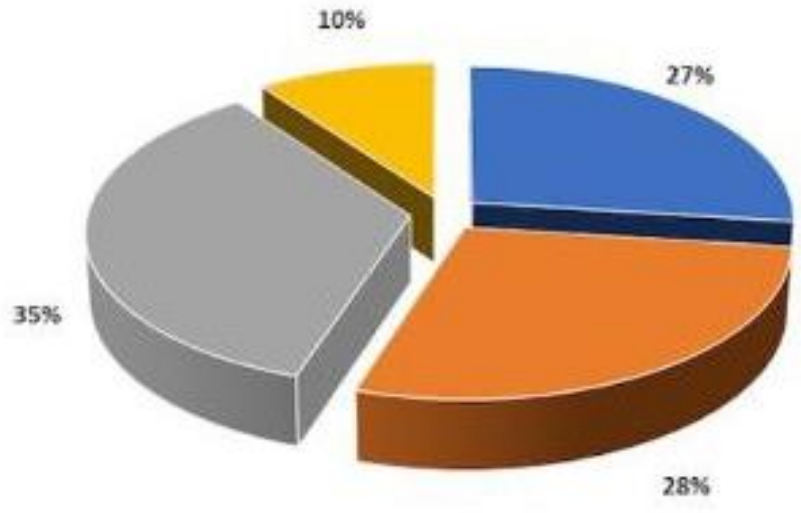

Рис. 1.4. Знайомство з PAM-системами у країнах СНД (27% - використовують; 28% - вивчали, але не використовують; 35% - знають загальні принципи; 10% - нічого досі не чули).

Такі цифри свідчать про те, що рівень ознайомленості та знань загальних

принципів PAM перевищує реальний досвід експлуатації даних рішень. Така відсоткова різниця між частиною країн Америки і Європи, та часткою країн СНД у застосуванні PAM-систем залежить від саме географічної сфери діяльності організації, бо тим чи іншим чином останні підлягають під відповідність стандартам NIST SP 800-53, GDPR або ISO 27001, що включають обов'язкові засоби контролю для безпечного керування привілейованими користувачами. [17] Таким чином недостатньо розвинена практика розповсюдження PAM призводить до того, що власники бізнесу не мають уявлення, що і для чого роблять привілейовані користувачі [4] у корпоративному середовищі компанії.

Відтак зростаюча потреба у захисті привілейованого доступу зумовлює стрімкий розвиток ринку рішень PAM. Згідно з даними Allied Marked Research [18] у 2020 році ринок оцінювався у 2,47 міль'ярда доларів, а до 2030 року очікується його зростання до 13,37 міль'ярдів доларів (див. Рис.1.5).

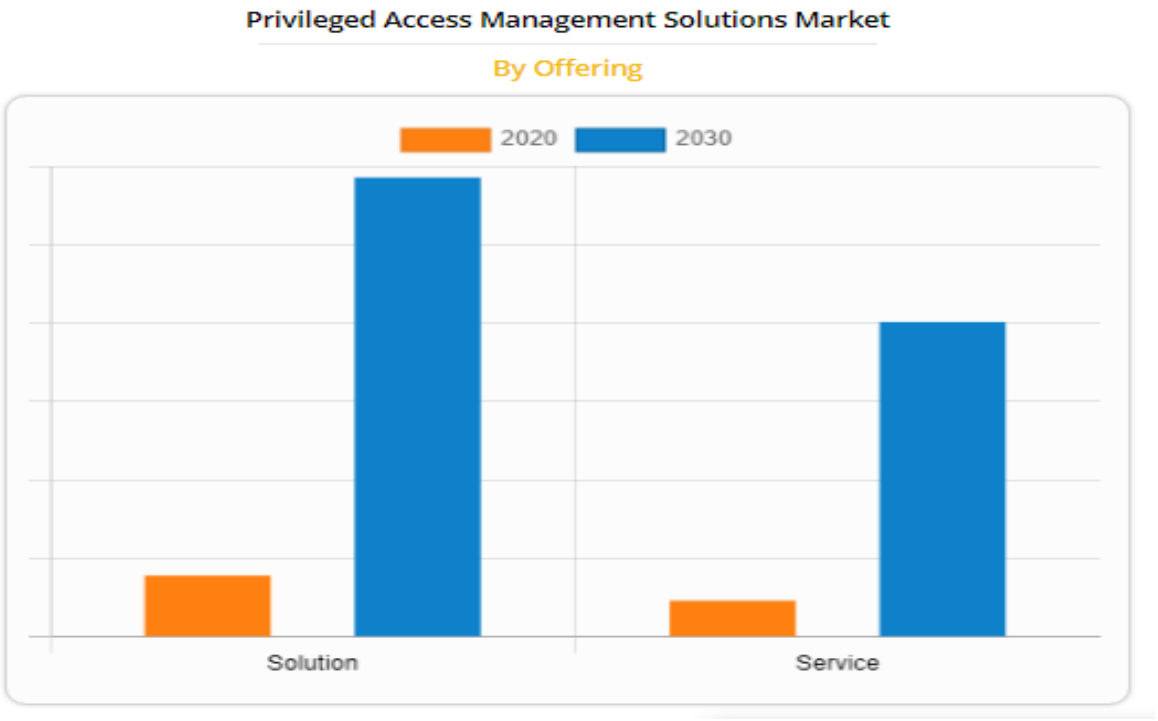

Рис. 1.5. Ринок рішень PAM

Окрім того опитування, проведене Delinea показало, що 21% компаній вже запровадили керування привілейованим доступом саме у хмарі або ж планують зробити це найближчим часом. Ще 26% планують перейти з локального PAM на хмарне рішення. [19] Така тенденція свідчить про

перехід бізнесу до хмари і ріст попиту на хмарні послуги, з чого випливає розуміння, що середовища постачальників хмарних технологій реалізують унікальні підходи до керування привілейованими доступами. За даними IDG 2020 року 90% компаній мали певну частину своєї інфраструктури у хмарі. Такий вибух хмарних сервісів призвів до поширення привілейованих облікових записів, що зумовлює необхідність переходу до хмари і PAM, тому що рішення для контролю доступу вже сприймаються як необхідне та належне. Відтак, хмара – це подальша перспективна стратегія розвитку для PAM.

Нижче наведено огляд та порівняння провідних доступних PAM рішень (табл), як хмарних, так і локально встановлених систем. Серед характеристик розглядались наявність: мультифакторної автентифікації, сховища паролів, управління паролями, управління обліковими записами, запис сесій, контроль доступу, можливість проведення аудиту, моніторинг дій користувачів, управляння привілеями, аналіз загроз та можливість пробного використання, проведення пілотних тестів. Окрім того порівняння технологій представлених провідних вендорів проводилось і за можливістю вирішення наступних проблем: несанкціонований доступ, відсутність контролю доступу, витік конфіденційної інформації, загрози хакерських атак, пошкодження даних, втрати доступу до даних, невідповідність вимогам. Також важливим аспектом була можливість скорочення витрат та забезпечення безперервності бізнесу. Не менш важливим для організації у виборі тієї чи іншої технології є визначення залучених співробітників, котрі займатимуться як обслуговуванням, налаштуванням, так і адмініструванням, тому розглядалась причетність таких ролей, як: виконавчий директор, IT директор, керівник відділу ІБ, менеджер з ІБ. І серед організаційних особливостей розглядалась область покриття даної системи відділів компанії: відділу ІБ та співробітників будь-якого іншого відділу, котрий має доступ в Інтернет.

Таблиця 1.1

Порівняння технологій PAM провідних вендорів

	ARCON	**BeyondTrust**	CYBERARK	FUDO	Hitaci ID	ONE IDENTITY	THYCOTIC	WALLIX
Характеристики								
Мультифакторана автентифікація	+	N/A	+	+	+	+	+	N/A
Сховище паролів	+	+	+	+	+	+	+	+
Управління паролями	+	+	+	+	+	+	+	+
Управління обліковими записами	+	+	+	N/A	N/A	+	+	+
Запис сесій	+	+	+	+	+	+	+	+
Контроль доступу	+	+	+	N/A	+	+	+	+
Проведення аудиту	+	+	+	N/A	+	+	+	+
Моніторинг дій користувачів	+	+	+	+	+	+	+	+
Управління привілеями	+	N/A	N/A	N/A	N/A	+	+	N/A
Аналіз загроз	N/A	+	+	N/A	N/A	N/A	N/A	N/A
Безкоштовний пробний період	+	+	+	+	+	+	+	+
Проблеми, що вирішують								
Несанкціонований доступ до IT систем та диним організації	+	+		+	+	+	+	+
Відсутність контролю доступу до інформації	+	+		+	+		+	+
Витік або ризик витоку конфіденційної інформації	+	+	+	+	+	+	+	+
Загрози хакерських атак	+	+	+	+	+	+	+	+
Ризик втрати та пошкодження даних	+	+	+	+	+	+	+	+
Ризик втрати доступу до даних та IT систем	+	+	+	+	+	+	+	+
Невідповідність вимогам IT безпеки	+	+	+	+	+	+	+	+

Продовження таблиці 1.1.

	ARCON	**BeyondTrust**	CYBERARK	FUDO	Hitaci ID	ONE IDENTITY	THYCOTIC	WALLIX
Цінності								
Скорочення витрат	+	+	+	+	+	+	+	+
Безпека і неперервність бізнесу	+	+	+	+	+	+	+	+
Ролі зацікавлених співробітників								
Виконавчий директор	+	+		+	+	+	+	+
IT директор	+	+	+	+	+	+	+	+
Керівник відділу ІБ	+	+	+	+	+	+	+	+
Менеджер з ІБ	+	+	+	+	+	+	+	+
Організаційні особливості								
Відділ ІБ	+	+	+	+	+	+	+	+
Співробітники з доступом в Інтернет		+	+		+	+		

Провівши дане порівняння, доцільно зазначити, що одними з найкращих постачальників PAM рішень є: ARCON, BeyondTrust, ONE IDENTITY та THYCOTIC, котрі являють собою найкраще поєднання інструментів та технологій захисту, контролю та моніторингу доступу до критично важливої інформації та ресурсам організації. PAM системи даних вендорів додатково включають: управління паролями загального доступу, управління привілейованими сеансами, управління привілейованими правами постачальників та управління доступом до додатків, що є переважаючими характеристиками при виборі даної технології компаніями.

Для проведення подальшої роботи було обране рішення PAM від вендора BeyondTrust, що є провідним постачальником на ринку управління привілейованим доступом. У своєму магічному квадранті привілейованого доступу за 2018 рік керівництво дослідницької компанії Gartner назвало BeyondTrust лідером у всіх категоріях рішень: від встановлення та застосування справжніх найменших привілеїв у системах Windows, Mac, Unix та Linux до автоматизації керування паролями і сесіями для забезпечення віддаленого

доступу співробітникам і третім сторінам, а також для інтеграції систем Unix, Linux і macOS з Microsoft Active Directory та аудиту діяльності адміністратора. BeyondTrust об'єднує ці можливості в єдину інтегровану платформу (див. Рис.1.6), яка діє як центральний менеджер політики та основний інтерфейс звітності.

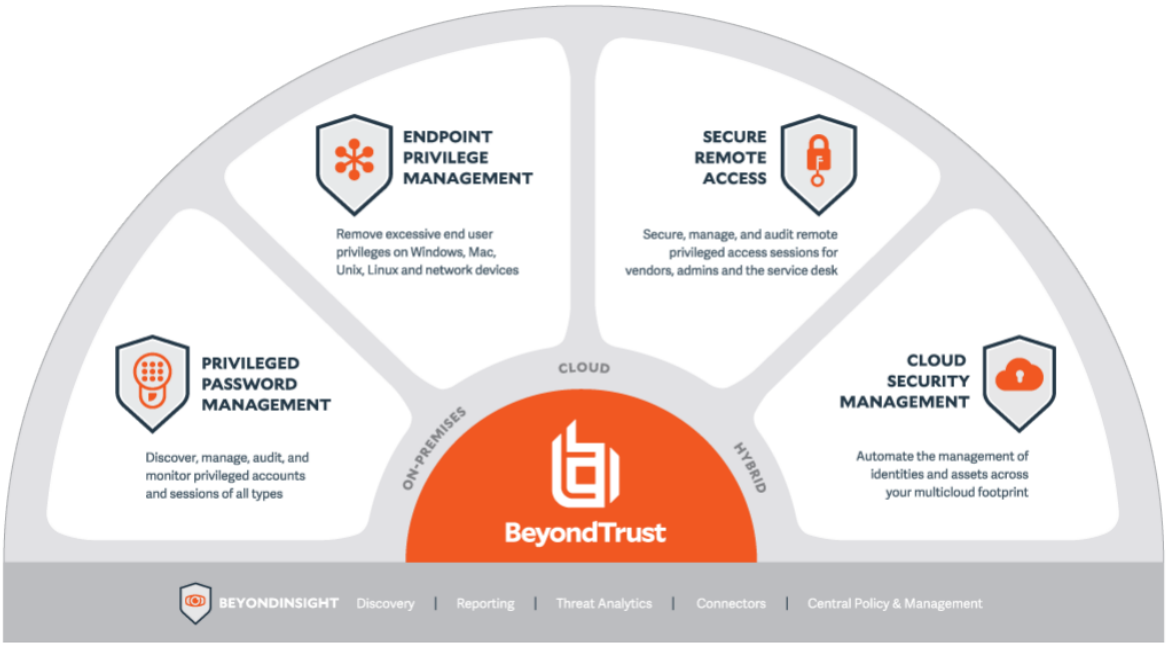

Рис. 1.6. Платформа BeyondTrust Privileged Management

Аналітики також визнають BeyondTrust лідером інновацій та революційного PAM, оскільки даний вендор, є першим хто:

- надав рішення з найменшими привілеями для Microsoft Windows;
- надав рішення з найменшими привілеями для Apple macOS;
- надав рішення для керування привілеями кінцевої точки, яке запроваджує інтелектуальний механізм захисту від несанкціонованого доступу;
- інтегрував надійну безпеку віддаленого доступу, яка справді поширює найкращі практики PAM на постачальників і віддалених працівників;
- запропонував інтегровану платформу для всіх основних випадків використання PAM на всіх основних платформах (Windows, macOS, Unix, Linux);
- надав платформу PAM, доступну на AWS Marketplace, вперше доступну на Microsoft Azure Marketplace і вперше доступну у Google Cloud.

Рішення та платформа BeyondTrust розроблені для забезпечення інтеграції з інструментами сторонніх розробників, серед яких:

- міжмережеві екрани наступного покоління і SIEM для кореляції ризиків і підвищення ефективності рішення;
- системами керування доступом до особистих даних;
- рішення для керування ідентифікацією (Sailpoint тощо);
- платформи Service Desk, допомагають посилити безпеку та підвищити продуктивність IT-довідкових служб.[23]

На вибір даної PAM системи також повпливала велика кількість задоволених клієнтів, а саме понад 20 тисяч у понад 80 компаніях.

Призначення, можливості, архітектура та функціонал даного PAM рішення буде розглядатись у наступних розділах даної роботи.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ BEYONDTRUST PRIVILEGE MANAGEMENT

2.1. Призначення, можливості та функції BeyondTrust Privilege Management

В реаліях сьогодення віддалена робота стала невід'ємною частиною функціонування бізнесу. І віддаленим співробітникам потрібен доступ до ресурсів компанії для виконання своїх службових обов'язків. Окрім того, перехід до різних хмарних моделей став ключовим для переходу на віддалених доступ та роботи з будь-якого місця. При такому підході важливо враховувати, щоб наданий співробітнику доступ не став загрозою кібербезпеки компанії, а заходи безпеки які функціонують в компанії локально часто не є достатніми для їх використання в хмарному середовищі. [24] У міру того, як середовище стає все більш децентралізованим і зростає складність у його контролі звичайними засобами захисут, побудова захисту периметру повинна розглядатись з точки зору того, що зловмисник вже присутній в середині. Відтак вимоги обмеження доступу до ресурсів компанії та їх мінімальний об'єм стають головним завданням в організації захисту, побудові віддаленого доступу і централізованому управлінні привілеями. Оскільки останні становлять найвищий ризик і представляють пріоритет безпеки, бо скомпрометований обліковий запис і пов'язані з ним дані є найпоширенішими векторами атак. Таким чином, масштаб управління всесвітом привілеїв вимагає комплексного, універсального підходу, а не купу інструментів, кожен з яких допоможе керувати лише їх частиною. [25]

BeyondTrust Universal Privilege Management реалізує новий підхід до управління привілеями за допомогою єдиної платформи для виявлення, захисту та перевірки кожного привілейованого облікового запису, активу та сеансу в усій інфраструктурі компанії, будь то локальне, хмарне чи її гібридне розгортання.

Основними можливостями та функціями даної платформи є:

- Централізоване адміністрування — постійне виявлення та інвентаризація хмарних, фізичних та віртуальних середовищ і їх складових, з подальшим групуванням для узгодженості управління привілеями на базі рольового доступу.
- Комплексний аудит і моніторинг будь-якого привілейованого об’єкту та його облікових даних — розпізнавання поведінки об’єкта та незвичних дій і сповіщення про можливі порушення безпеки.
- Привілейований пароль і управління привілейованим сеансом — належне використання облікових даних відповідно до прийнятої парольної політики, яка визначатиме: складність та унікальність паролів, термін дії, зміну, видалення всіх паролів за замовчуванням, приховування паролів, зберігання в сесіях. [25] Продукт вводить облікові дані безпосередньо в сеанси віддаленого доступу, завжди приховуючи їх від користувача. [14]
- Безпека та аудит віддаленого доступу - захист, управління та перевірка постачальників, внутрішніх привілейованих користувачів та віддалених з використанням списків контролю доступу, зонування мережі та сегментації хмари. [25] Рішення також надає можливість проксі-доступу до RDP, SSH, хмарних екземплярів і програм Windows/Unix/Linux. [14]
- Найменші привілеї та мінімальний час — управління необхідними і достатніми привілеями для кінцевого об’єкта, “точно та вчасно” здійснюючи їх підвищення протягом необхідного часу. Динамічна модель доступу зменшує поверхню загрози та обмежує можливість отримання привілей, ескалацію атак. Це позбавляє користувачів необхідності здійснювати автентифікацію з правами адміністратора та усуває можливість використання адміністративних привілей.
- Безпечна інфраструктура розробки — забезпечення видимості, контролю та безпеки IT, розмежування середовищ розробки, тестування та виробництва.
- Моніторинг та управління сесіями з привілейованим доступом — забезпечення безпеки, проведення аудиту та звітність про привілейовану

діяльність усіх запущених сеансів, автоматизація робочих процесів.

Відтак BeyondTrust усуває ключові прогалини в безпеці гібридного середовища, видимості та управлінні, а також здійснює захист за допомогою:

- постійного виявлення та підключення привілейованих облікових записів і хмарних екземплярів;
- застосування найкращих практик безпеки облікових даних для кожного облікового запису, включаючи впровадження архітектур нульової довіри;
- зменшення кількості користувачів з привілейованим доступом;
- обмеження привілеїв доступу будь-якого користувача, програми, служби чи активу;
- запобігання та пом'якшення людських помилок у привілейованому доступі;
- звуження вікна часу, протягом якого привілеї можуть бути виконані, і таким чином зловживаними, застосовуючи принцип своєчасного доступу;
- примусової сегментація хмарного середовища та віддаленої безпеки/проксі-сервера доступу до хмарних консолей керування та обчислювальних ресурсів;
- надійного керування та моніторингу кожного привілейованого сеансу та забезпечення сертифікації на відповідність нормативним вимогам;
- надання єдиної централізованої платформи для всіх видів діяльності з керування привілеями створеної для інтеграції з іншими засобами безпеки. [25]

Основними сценаріями використання рішення BeyondTrust є незалежні та легко інтегровані варіанти використання [24]:

- облік привілейованих облікових записів;
- впровадження принципу найменших привілей на кінцевих пристроях;
- впровадження принципу найменших привілей на серверах;
- репутація додатків;

- віддалений доступ;
- мережеві пристрої та інтернет речі;
- віртуалізація та хмари;
- безпечна розробка;
- інтеграція привілейованих облікових записів з іншими інструментами;
- інтеграція з IAM рішеннями.

Тож ключовими перевагами платформи BeyondTrust є :

- пом’якшення зовнішніх та внутрішніх загроз;
- забезпечення підзвітності за допомогою моніторингу та запису сеансу, реєстрації натискань клавіш та аудиту у реальному часі;
- захист IT-середовища — локальної, хмарної, гібридної архітектури;
- спрощення шляху проходження аудитів, дотримання урядових і галузевих стандартів та інших вимог звітності;
- забезпечення безпеки та продуктивності працівників та партнерів;
- сприйняття нових технологій та бізнес-ініціатив.

2.2. Компоненти та архітектура рішення Beyondtrust Privilege Management

Рішення BeyondTrust Privilege Management — уніфіковане управління привілеями в усьому хмарному та локальному середовищі. Привілейоване керування паролями, управління привілеями кінцевих точок і безпечний віддалений доступ можуть бути розгорнуті окремо, або об’єднанням кількох рішень BeyondTrust для отримання максимального привілею, контролю і зниження ризику (див. Рис.2.1). Кожним із рішень можна керувати через BeyondInsight консоль, яка централізує адміністрування, аудит звітності тощо. [25]

Тож платформа BeyondTrust надає чотири універсальні інтегровані рішення, які підвищують продуктивність бізнесу. Серед них:

- Privileged Password Management – рішення котре допомагає знаходити, підключати, керувати та перевіряти кожен привілейований обліковий запис та відслідковувати кожен сеанс.
- Endpoint Privilege Management – рішення котре допомагає надавати необхідні привілеї кожному користувачу чи додатку лише на визначений час.
- Secure Remote Access – рішення котре дозволяє керувати та контролювати привілейований віддалений доступ для співробітників та постачальників. [26]
- Cloud Security Management – автоматизоване управління безпекою облікових записів та активів у багатохмарному середовищі.

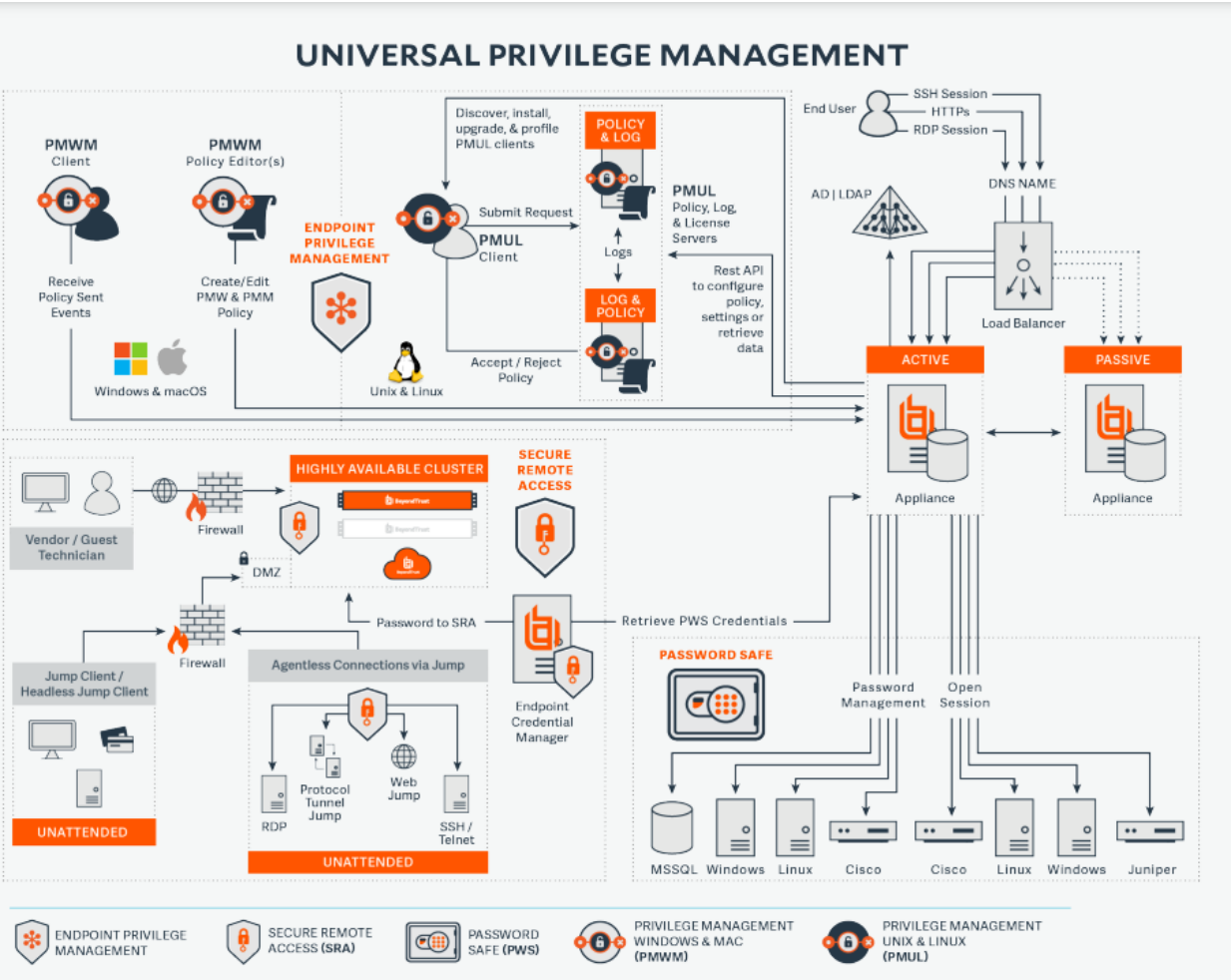

Рис. 2.1. BeyondTrust PAM архітектура

Підхід BeyondTrust Universal Privilege Management надає повний та масштабований спосіб захисту привілейованих облікових даних, записів,

паролів, секретів та сеансів, забезпечуючи компаніям додаткову безпеку, контроль та моніторинг покриваючи основні сценарії використання. [27]

2.3. Призначення, архітектура рішення Privileged Password Management та можливості щодо адміністрування

Рішення BeyondTrust Privileged Password Management автоматично визначає та бере під контроль всі типи привілейованих облікових записів, що використовуються в організації. Взяття облікових записів під контроль має на увазі те, що система змінює паролі та ключі облікових записів співробітників, вендорів, сервісів, служб та вшитих в код облікових записів, на виклики API, підсилює сегментацію за рахунок розподілу привілей та відповідальності. А також веде моніторинг та керування кожним привілейованим сеансом здійснюючи аналіз потенційних загроз і збір журналу аудиту привілейованих дій. [24]

Privileged Password Management складається з трьох основних компонентів:

1. Password Safe об’єднує привілейований пароль і керування привілейованим сеансом, надаючи комплексне виявлення, керування, аудит і моніторинг (див. Рис.2.2) для будь-якого привілейованого облікового запису чи даних об’єкта. [25]

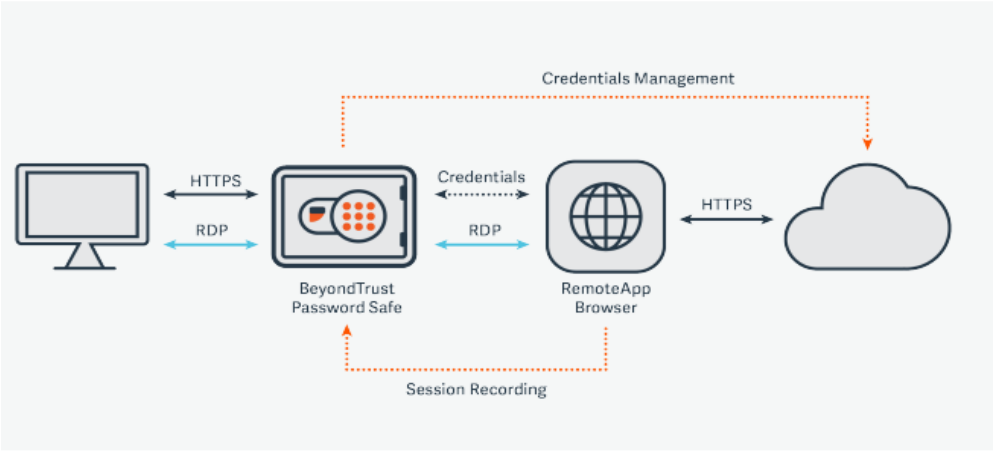

Рис. 2.2. Password Safe надає комплексне виявлення, керування, аудит і моніторинг

Крім того, BeyondTrust Password Safe може виступати в якості проксі служби доступу до хмари для привілейованих облікових записів, з метою забезпечення контролю доступу та аудиту на глибшому рівні, ніж це доступно за допомогою власних елементів керування та загального протоколу віддаленого доступу. (див. п.2.6)

Можливості адміністрування [27]:

- Управління привілейованими паролями та сеансами — забезпечення відповідності вимогам регуляторів та проведення розслідувань. Password Safe та BeyondTrust Privileged Remote Access забезпечують безпечний доступ сторонніх вендорів за допомогою єдиного підходу до забезпечення безпеки підключення та автоматичної перевірки привілейованих облікових даних та повного запису сеансу доступа.
- Сканування, ідентифікація, групування всіх ресурсів та автоматичне маркування облікових даних — забезпечення автоматичного перехоплення управління привілейованими обліковими записами. Password Safe включає в себе інтеграцію з SailPoint IdentityIQ, що дозволяє компаніям ефективно керувати доступами користувачів з привілейованими та непривілейованими обліковими записами.
- Контроль привілейованих облікових записів, додатків, SHH-ключів, хмарних облікових записів адміністраторів — забезпечення контролю доступу та прийняття рішення про його надання на основі оцінки поточного стану.
- Аналітика загроз привілейованого доступу — забезпечення співставлення характеристик та попередження про підозрілу поведінку. Password Safe мінімізує ризики слабкої чи неконтрольованої парольної політики, що забезпечує безпечне зберігання хмарних адміністративних облікових даних до Azure, Amazon, Google, Rackspace, та GoGrid, до соціальних мереж: Facebook, LinkedIn та Twitter.

2. Cloud Vault являє собою хмарне сховище для зберігання привілейованих облікових записів

Можливості адміністрування [27]:

- Управління паролями — безпечне зберігання, вилучення будь якої комбінації облікового логіну/пароля чи SSH-ключів, пов’язаних з конкретним користувачем чи адміністративним обліковим записом.
- Надання доступу привілейованим користувачам — швидкий доступ до систем без втрати часу на відслідковування облікових даних.
- Управління привілейованими сеансами — безпека протягом всього сеансу віддаленого доступу до будь-яких пристроїв з будь-якого місця. Без розкриття привілейованих паролів. А інтеграція Cloud Vault з Privileged Remote Access усуває необхідність запам’ятовувати паролі та логіни кінцевим користувачам та зберігає записи журналів для кожного віддаленого сеансу.
- Підвищена безпека, знижені ризики кібератак — аудит привілейованих користувачів, та створення єдиного шляху для доступу.
- Виконання вимог регуляторів — моніторинг сеансів привілейованих доступів та ведення журналу даних сеансів.
- Безпека хмарних та віртуальних систем — управління привілейованим доступом до бізнес ресурсів, що використовують консолі управління на основі веб-інтерфейсів.

3. DevOps Secret Safe – окремий додаток, розроблений на основі мікросервісів, що використовує контейнери Docker і розгортається за допомогою Kubernetes. Рішення призначене для роботи в середовищі розробки та зниження ризиків розкриття секрету.

Можливості адміністрування [27]:

- Централізоване управління секретами — сховище для всіх секретів та привілейованих облікових даних об’єктів.
- Висока доступність — мінімізація ризиків простою.
- Автоматизований аудит та ведення журналу — відслідковування всіх дій над секретами для контролю звернень до ресурсів.
- Інтерфейс командного рядка — полегшена взаємодія з API.
- Вбудовані засоби інтеграції з інструментом DevOps – захист та управління секретами додатків та розповсюджених інструментів DevOps.

2.4. Призначення, архітектура рішення Endpoint Privilege Management та можливості щодо адміністрування

Загалом технології управління дозволяють організаціям контролювати які дії можуть виконувати кінцеві користувачі. У багатьох компаніях користувачі мають повні адміністративні права, які дозволяють їм встановлювати та запускати невідомі програми. Таким чином існує ризик зараження зловмисним програмним забезпеченням, котре працюватиме з підвищеними привілеями та обходитиме елементи керування безпекою. Тож надаючи права локального адміністратора кінцевим користувачам, компанії ставлять у зону високого ризику власні конфіденційні дані. За допомогою рішень управління привілеями кінцевих точок підвищується гарантія того, що працюють лише довірені програми з найнижчими привілеями, так як організації можуть видалити локального адміністратора та призначити мінімальні привілеї. За Gartner, керування привілеями кінцевих точок використовує керування привілеями і керування додатком, щоб визначити, по-перше, чи може програма працювати, а по-друге, як (за яких умов привілею) користувач може з нею працювати».

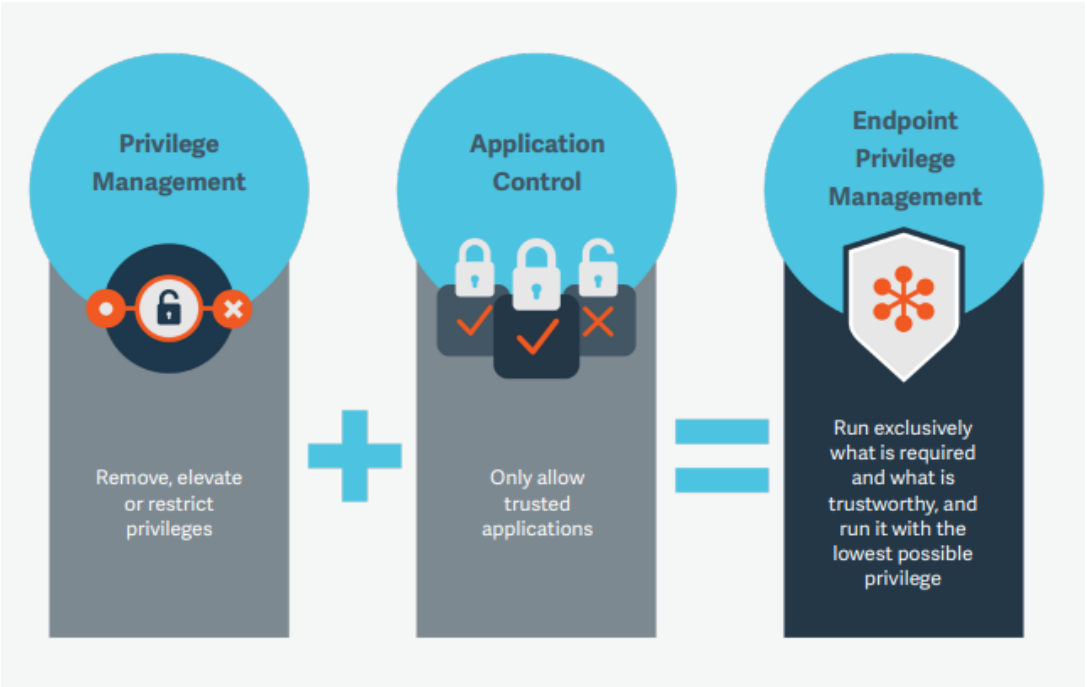

Рис.2.3. Управління привілеями кінцевих точок

Відтак управління привілеями кінцевих точок (див. Рис.2.3) — це процес надання достатньої кількості співробітникам доступів, щоб залишатися продуктивними у своїх ролях, не надаючи їм повних прав адміністратора над IT-системою.

Окрім того управління привілеями кінцевих точок заповнює прогалини в забезпеченні безпеки кінцевих точок (див. Рис.2.4) між антивірусними інструментами та рішеннями Endpoint Detection and Response. На кінцевих точках повинні бути встановлені антивірусний захист та брандмауери, оскільки вони є готовими рішеннями та можуть пом'якшити багато відомих атак. Однак, за даними Ponemon, 60% атак є промахами, що складаються з атаки нульового дня, і це є значною проблемою, враховуючи кількість нових зловмисних програм з’являються на день - згідно з Avtest.org даний показник досягає позначки у 350 000.

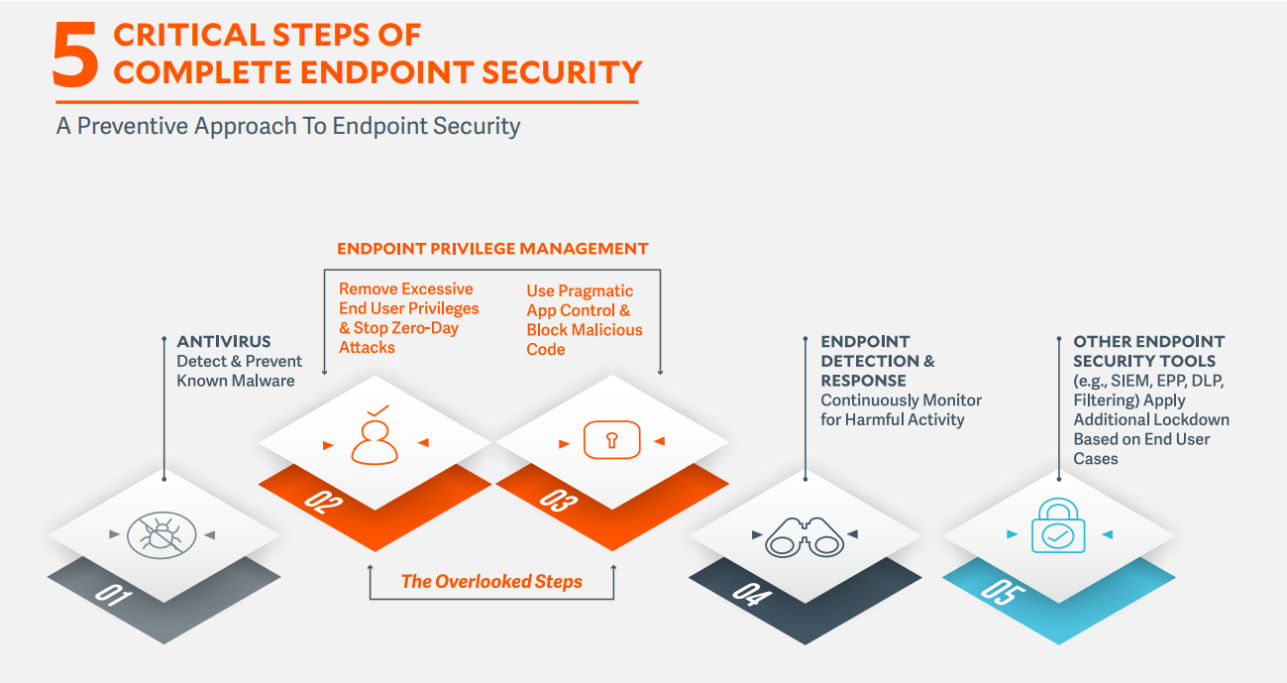

Рис.2.4. Кроки забезпечення безпеки кінцевих точок

BeyomdTrust Endpoint Privilege Management – інструмент динамічного управління мінімально можливими та необхідними привілеями при реалізації доступу до кінцевих точок будь-якого типу. Рішення дозволяє видаляти права адміністратора та впроваджувати оренду привілей, підвищувати права,

прибирати зайві, впроваджувати контекстні правила та багатофакторну автентифікацію.[24]

Окрім того, інтеграція пристроїв Series Appliance, BeyondInsight і Privilege Management є рішенням (див. Рис.2.5) для керування привілеями, яке передає дані про кінцеві точки та політики на централізовану консоль керування BeyondInsight з можливостями звітування та аналітики, необхідними для зниження ризику, підвищення безпеки та надання користувачам змоги ефективної роботи. Кінцеві точки керування привілеями та пристрій U-Series-BeyondInsight обмінюються даними за допомогою сертифікатів TLS для автентифікації обох сторін. Служба подій використовується для зв’язку між Privilege Management і BeyondInsight за допомогою порту 443. Події з Privilege Management надсилаються до BeyondInsight за допомогою цієї служби. Зв'язок по цьому каналу захищений, за допомогою сертифіката клієнта, від кінцевої точки до пристрою, де розміщено BeyondInsight. Жодні порти не повинні бути відкриті на стороні клієнта. TCP-порт 1443 необхідний для підключення бази даних SQL Server від сервера подій до сервера, на якому розміщено базу даних.

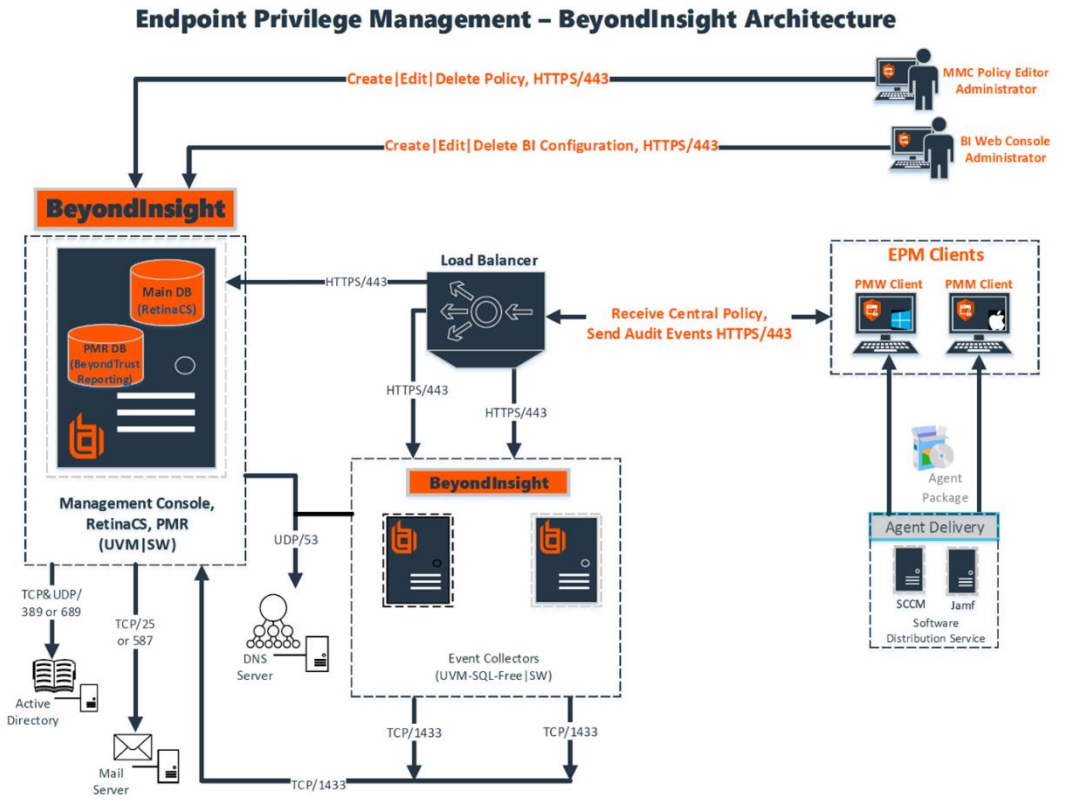

Рис. 2.5. Архітектура BeyondInsight - Privilege Management

Загалом, рішення Endpoint Privilege Management складається з трьох компонентів:

1. Privilege Management для Windows та Mac – рішення, яке представляє собою агента для управління адміністративними правами на робочих станціях, де користувачу не потрібні повні адміністративні права. [26]

Основні характеристики:

- вбудовані політики на основі досвіду впровадження на кінцевих точках;
- видалення привілей адміністратора без загроз продуктивності;
- встановлені за змовчуванням правила покривають більшу частину випадків використання;
- запис поведінкових даних для покращення політик;
- єдиний сценарій використання з робочими станціями та серверами.

Можливості адміністрування [27]:

- Шаблони для швидкого старту — видалення всіх адміністративних прав у всіх користувачів.
- Захист додатків — встановлені шаблони зупиняють, спрямовані на додатки, атаки, перехоплюючи скрипти та інфіковані вкладення в повідомленнях електронної пошти.
- Контроль вкладень — обробка “білих списків”.
- Інтеграція з іншими засобами захисту — швидкий час входу в експлуатацію та інтеграція зі сторонніми вендорами.
- Аналіз загроз, пов’язаних з привілеями — оцінка ризиків кінцевих точнок, на основі взаємодії користувача з ресурсами.
- Аудит та звітність — журнал контролю всіх дій користувача.

2. Privilege Management для Unix, Linux та мережевих пристроїв є рішенням контролю використання привілей. Ядром даного рішення є сервер авторизації, котрий обробляє запити на використання привілей на основі політик ідентифікації та використання привілей. Рішення надає можливість об’єкту використовувати лише необхідні привілеї для необхідних серверів. [26]

Управління привілеями на кінцевих точках під управлінням Unix, Linux містить основні компоненти та кроки (див. Рис.2.6):

- встановлений на сервері клієнт, для запуску команд з підвищеними привілеями та надсиланням їх на другий компонент;
- сервер політик, котрий оцінює політики і на основі бізнес-правил приймає рішення про дозвіл запуску команд;
- журнал подій, де зберігаються всі дії з командами;
- модуль запису сеансів, котрий запускає запис сеансу на сервері політик до запуску команд з підвищеними привілеями;
- клієнт, що запускає команду від імені користувача.

Така архітектура забезпечує централізоване управління політиками та аудит. Замість захоплення записів журналу аудиту на комп'ютері користувача з адміністративним доступом, система захоплює записи на сервері, на якому авторизується користувач та котрий відповідає за підвищення привілей.

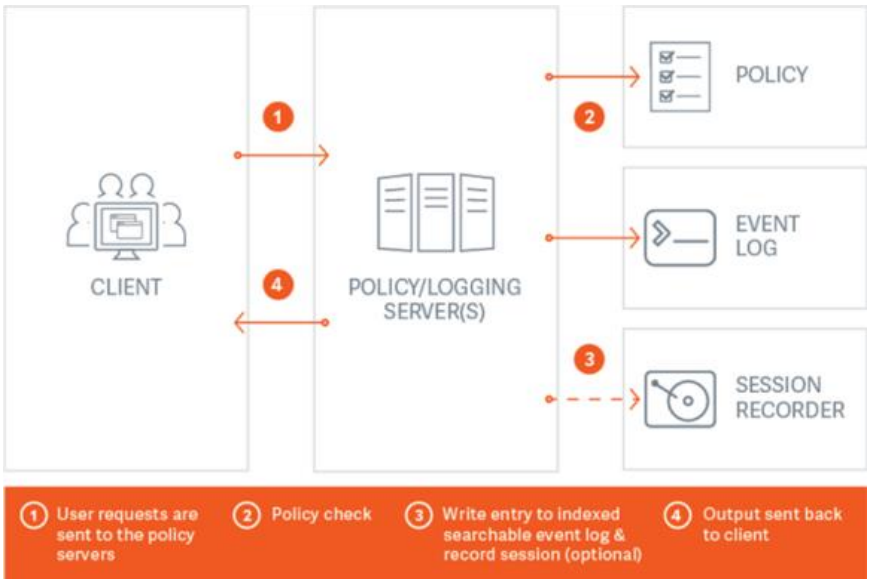

Рис. 2.6. Управління привілеями на кінцевих точках під управлінням Unix, Linux

Можливості адміністрування [27]:

- Аудит та управління — аналіз поведінки користувача з використанням збору, зберігання, запису сеансів привілейованого облікового запису.
- Налаштування найменших привілей — управління підвищенням

привілей на основі політик.

- Контроль віддалених системних додатків — віддалений запуск команд та сеансів на основі правил без додаткової авторизації користувача з адміністративним обліковим записом.
- Динамічна політика доступу — прийняття рішення про підвищення привілей на основі факторів часу, дня, статусу, місця розташування.
- Моніторинг цілісності файлів та політик — аудит цілісності файлів політик, систем, додатків, даних.
- Аналітика та звітність про загрози — кореляція поведінки користувача з даними про вразливості ресурсів.

3. Active Directory Bridge додає до Active Directory аутентифікацію Kerberos для середовищ Unix, Linux та Mac та дозволяє реалізувати єдиний вхід на даних платформах.

Можливості адміністрування [27]:

- Використання облікових записів AD для доступу до Unix, Linux та Mac систем.
- Управління груповими політиками.
- Аудит декількох подій в реальному часі.
- Перехід користувачів до віддаленого доступу без необхідності повторного введення облікових даних.
- Об’єднання каталогів для спрощення управління багатокомпонентними середовищами.

2.5. Призначення та архітектура рішення Secure Remote Access та можливості щодо адміністрування

Secure Remote Access дозволяє контролювати доступ співробітників, вендорів, служб підтримки з використанням принципу найменших привілей. Рішення надає можливість здійснювати віддалений доступ та використовує сховище паролів для виявлення та управління привілейованими обліковими

даними.[26]

Дане рішення створює одноразові облікові дані для запуску сеансів, не розкриваючи паролів, мінімізуючи ризик компрометації. Оскільки забравши можливість віддаленого з'єднання через VPN (див. Рис.2.7): повним доступом до мережі, відкриттям портів в брандмауерах, створюючи вразливості; стає можливим здійснення управління привілеями, контролю кількості сеансів та часу доступу. Такий контроль за орендованими привілеями дозволяє керувати тим, які команди можуть запускатись користувачем. [24]

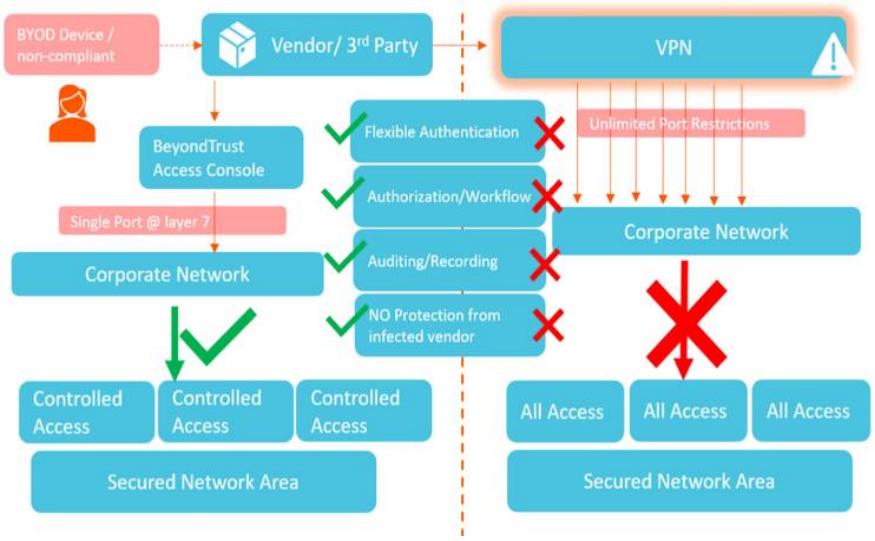

Рис.2.7. Secure Remote Access vs VPN

BeyomdTrust Secure Remote Access включає два рішення:

1. Privilege Remote Support дозволяє здійснювати технічну підтримку за будь-яких умов. Для вирішення технічних проблем інженер може переглядати екран віддаленого комп'ютера, надсилати повідомлення, вносити зміни в реєстр, надсилати файли. [24]

Можливості адміністрування [27]:

- Віддалений доступ та контроль.
- Ефективність та масштабованість — управління доступом до безлічі систем, підвищення безпеки бізнесу.
- Індивідуалізація та брендування — підтримка корпоративного бренду та індивідуальні процедури взаємодії з клієнтами.

- Адміністрування команд та дозволів — керування користувачами, ролями команди, налаштування сеансів з використанням принципу найменших привілей.
- Аудит та дотримання вимог регуляторів.
- Інтеграція з різними системами та інструментами управління паролями, а також створення власних інтеграцій.

2. Privilege Remote Access дозволяє контролювати доступ до критичних систем не змінюючи робочі процедури віддалених користувачів. [24] Рішення знижує необхідність запам’ятовувати чи сумісно використовувати облікові дані для доступу до систем, а паролі зберігаються в сховищі пристрою, а також легко інтегрується з групою Password Management.

Компанії використовують як локальну так і хмарну архітектуру для запуску критичних систем, відтак Privilege Remote Access забезпечує централізовану безпеку та керування доступом до всіх середовищ, включно з критичними системами в хмарі (Рис.2.8). Загалом рішення пропонує кілька варіантів доступу до хмарних середовищ: власний агент, який дозволяє вимкнути застарілі протоколи доступу; безагенний підхід, який використовує бастіонний хост і зберігає весь застарілий трафік локально; опція вбудованого браузера Chromium для ізоляції віртуального браузера, який буде єдиним авторизованим джерелом для всіх хмарних ресурсів. [25]

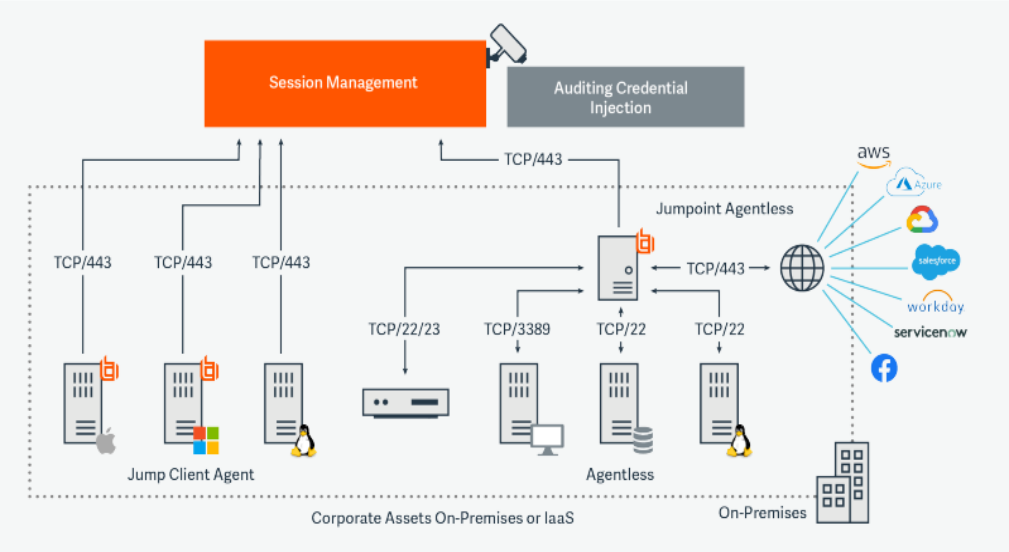

Рис.2.8. Архітектура Privilege Remote Access

Можливості адміністрування [27]:

- Захист доступу — попередження розповсюдження привілей та застосування найменших привілей для захисту IT-ресурсів.
- Інтеграція з рішеннями управління паролями.
- Робота в гібридних середовищах.
- Використання існуючих інвестицій в безпеку — підвищення безпеки IaaS-записів.
- Мобільний додаток / веб-консоль — доступ з будь якого мобільного пристрою чи веб-браузера.
- Аудит та виконання вимог регуляторів.

2.6. Призначення та архітектура рішення Cloud Security Management та можливості щодо адміністрування

Для обробки, зберігання, розміщення і розробки додатків все частіше використовуються віртуалізовані ЦОД та хмарні середовища. У хмарі існує безліч рівнів привілей для різних об’єктів. Платформа управління привілейованим доступом BeyondTrust разом з рішенням Cloud Security Management забезпечує надійну видимість і безпеку в усьому всесвіті хмари (IaaS, PaaS, SaaS).

З точки зору управління привілейованим доступом забезпечення безпеки хмарних ресурсів схоже на захист локальних, але з певними відмінностями:

- використання менеджера паролів для управління паролями, ключами лише в хмарних середовищах: паролями гіпервізорів, API та консолей;
- впровадження рішень для управління привілейованим доступом з контролем сеансів доступу до хмарних провайдерів з правами адміністратора чи суперкористувача;
- використання сховищ секретів для захисту секретів при змінах в DevOps у хмарах.

За допомогою Password Safe, можна заблокувати керування Azure/Office365 ролям Global Administrator, обмежуючи мережевий трафік лише самим рішенням. Однак Password Safe Cloud використовуватиме брокера ресурсів між Password Safe і цілями. На зображенні нижче (рис.2.9) показано, як локальні та IaaS реалізації рішення BeyondTrust працюють. [25]

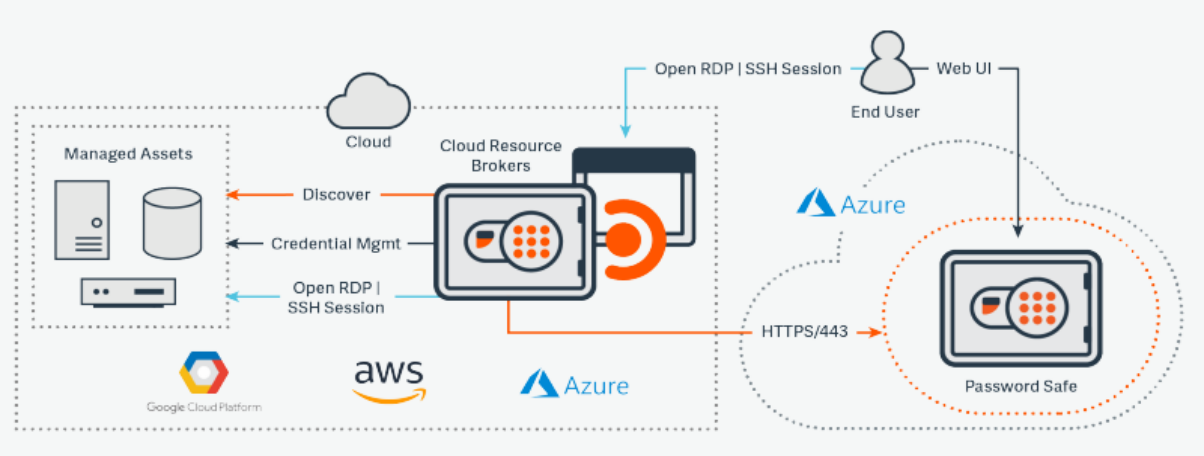

Рис.2.9. Архітектура Password Safe Cloud

Password Safe Cloud розміщено в Microsoft Azure, та його розгортання складається з:

- консолі управління на базі BeyondTrustCloud та порталу користувача Password Safe;
- брокерів ресурсів;
- локально розгорнутого агенту у мережі клієнта для реалізації локальних функцій.

Архітектура мережі (див Рис.2.10) побудована для захисту всіх точок входу, призначених клієнтам. Граничні шлюзи високої доступності та сегментовані мережеві компоненти виділені та налаштовані в BeyondTrust. Інфраструктура постійно контролюється, а перевірка вразливостей регулярно проводиться співробітниками внутрішньої безпеки та сторонніми групами безпеки. Доступ до консолі керування Azure, де керується конфігурація мережі/VNet, також сильно обмежений у межах BeyondTrust і доступний лише для тих, кому потрібен доступ до консолі. Весь вхідний трафік до сайту Password

Safe Cloud клієнта використовує стандартний зашифрований HTTP на порту 443. Локальний брокер ресурсів також спілкується з примірником Password Safe Cloud за допомогою 443, але додатково вимагає ввімкнення іншого конкретного трафіку.

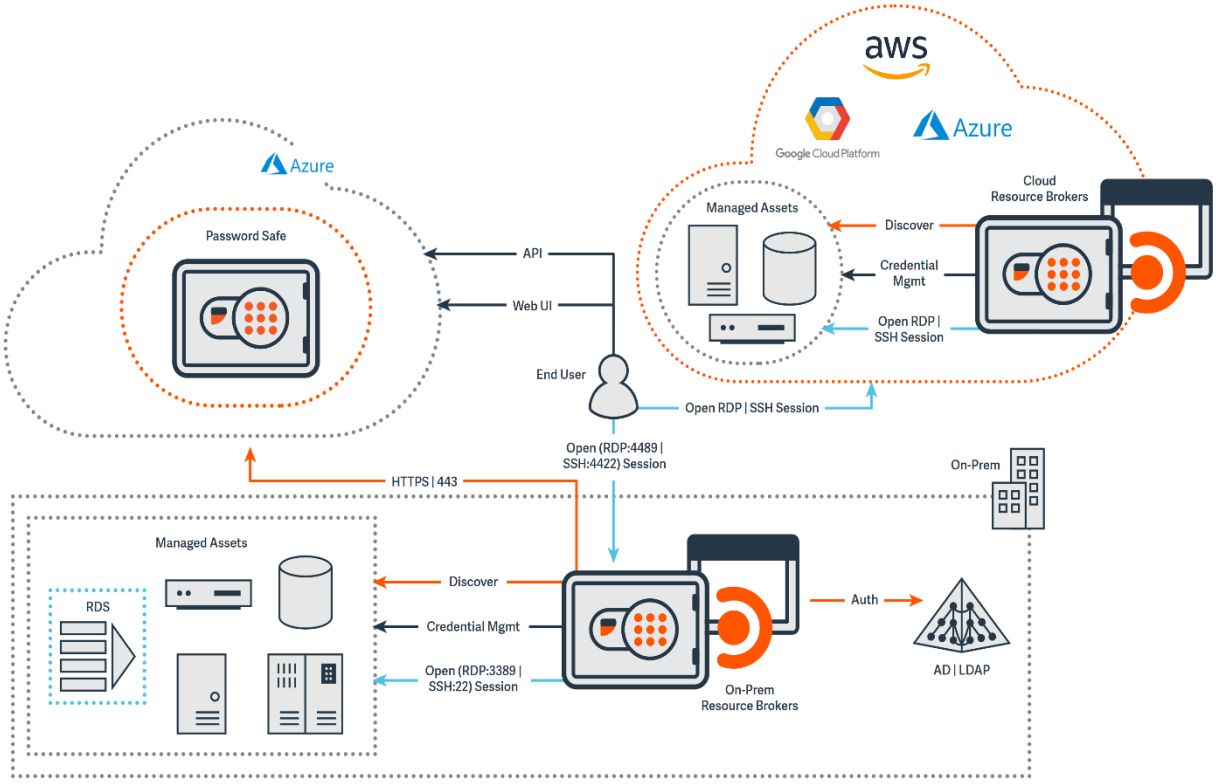

Рис.2.10. Архітектура розгортання Password Safe Cloud в Microsoft Azure

Відтак даний підхід гарантує, що весь доступ до хмарних активів сегментується, захищається, контролюється та перевіряється.

2.7. Вимоги до системи для інсталяції рішень BeyondTrust Privilege Management

Рішення BeyondTrust Privilege Management не висуває суворих системних вимог для інсталяції (див. Табл.2.1), окрім як версій операційних систем, бо є мультиплатформенним рішенням для усунення можливостей реалізації атак, видаляючи надмірні привілеї на Windows, Mac, Unix, Linux, мережевих пристроях та в хмарі.

Таблиця 2.1.

Системні вимоги для інсталяції рішень BeyondTrust Privilege Management

Підтримка платформ	Точкові рішення	Консоль
Windows	Windows 7 SP1 Windows 10 Windows 11 Windows Server 2008 SP2 - 2019	Windows 10 Windows 11 Windows Server 2016 - 2019
macOS	macOS 10.13 - 10.15 macOS 11 (Big Sur) x86 and xApple macOS 12 (Monterey)	macOS 10.13 - 10.15 macOS 11 (Big Sur) x86 and xApple macOS 12 (Monterey)
Linux	Fedora 31-32 RedHat Enterprise 8.2 Ubuntu 18.04 LTS, 20.04 LTS	Fedora 31-32 RedHat Enterprise 8.2 Ubuntu 18.04 LTS, 20.04 LTS
Мобільні пристрої		Apple iOS 12.0+ Android 6.0+
Віртуальні машини		Citrix XenDesktop 5, 7 VMWare View 5 VMWare Horizon 6, 7 Citrix XenApp 6.5, 7.5
Віртуальні пристрої	vSphere 5.0 - 6.7 Azure AWS - AMI Sharing Nutanix	
Автоматичні системи	Ноутбуки, настільні комп’ютери, сервери, банкомати, кіоски, POS-системи, Raspberry Pi тощо.	
Контроль доступу до хмари	Безпечне підключення та управління хмарною інфраструктурою, включаючи віртуальні машини Windows, Red Hat, CentOS і Ubuntu Linux на базі AWS, Azure, VMware та інших постачальників IaaS. Також підтримуються безголові конфігурації Linux.	
Мережеві пристрої	Маршрутизатори, комутатори та пристрої через SSH/Telnet	
Підтримка мов	Перегляд програм та інтерфейсів BeyondTrust англійською, голландською, французькою, німецькою, італійською, японською, російською, спрощеною китайською, польською та традиційною китайською. BeyondTrust підтримує міжнародні набори символів.	

3. ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ BEYONDTRUST PRIVILEGE MANAGEMENT

3.1. Розробка варіанта топології та визначення критичних точок в управлінні привілейованим доступом у корпоративній інформаційній системі

У ході даної роботи розглядалась топологія мережі, розроблена на основі реально існуючого підприємства, але дещо спрощена з метою збереження та не розголошення комерційної таємниці даного підприємства. Назву також було замінено на “Компанія”. Щоб не розкривати всіх деталей, щодо стану захищеності даного підприємства та всіх складових компонентів мережі, і не наражати на небезпеку, основний фокус уваги був зосереджений саме на привілейованому доступі користувачів, що відповідає обраній темі.

Організація “Компанія” є рекламною агенцією, котра співпрацює з вітчизняними клієнтами, та має на меті вийти на іноземний ринок. Організаційна структура агенції представлена (див. Табл.3.1) п’ятьма підрозділами з визначеною кількістю працівників на конкретних посадах, їх рівнями доступу (повний доступ до ресурсів та об’єктів, частково обмежений — право використовувати будь-які ресурси свого відділу і лише окремі ресурси інших з відповідним дозволами, обмежений — робота з обліковим записом користувача та наданими йому доступами) до мережевих ресурсів, конфіденційної інформації (1 - інформація про партнерів, клієнтів; 2 - діловодство, облік; 3 - перепустки, службові печатки; 4 - облікові записи, паролі; 5 — суми, платежі та грошові транзакції; 6 - середовища розробки та дизайну) та правами (звичайний користувач - user, адміністратор - admin), режимом роботи (локально, віддалено), використовуваними сервісами (хмарні, локальні) та робочими пристроями (корпоративні, власні), необхідністю виходу в Інтернет (є потреба, нема).

Таблиця 3.1.

Організаційна структура “Компанія”

Посада та кількість співробіт-ників	Режим роботи	Рівень доступу до мережевих ресурсів	Доступ до конфіденці йної інформації	Права в системі	Використо-вувані сервіси	Робочі пристрої	Необхід-ність виходу в Інтернет
Керівництво							
Директор	локально/ віддалено	повний	1, 3, 4, 5	admin	хмарні/лок альні	корпорат/ власні	є потреба
Секретар	локально/ віддалено	обмежений	2, 3, 4	user	хмарні/лок альні	корпорат/ власні	є потреба
IT-відділ							
Керівник	локально/ віддалено	повний	3, 4, 5, 6	admin	хмарні/лок альні	корпорат/ власні	є потреба
web-Дизайнер	віддалено	повний	4, 5, 6	admin	хмарні	власні	є потреба
web-Розробник	віддалено	повний	4, 5, 6	admin	хмарні	власні	є потреба
Системний адміністра-тор	локально/ віддалено	повний	3, 4	admin	хмарні/лок альні	корпоратив-ні	є потреба
Інженер ІС	локально/ віддалено	повний	3, 4	admin	хмарні/лок альні	корпоратив-ні	є потреба
Фінансовий відділ							
Головний бухгалтер	локально/ віддалено	частково обмежений	1, 2, 3, 4, 5	admin/ user	хмарні/лок альні	корпорат/ власні	є потреба
Спеціаліст (2)	локально/ віддалено	обмежений	1, 2, 4, 5	user	хмарні/лок альні	корпоратив-ні	є потреба
Діловод	локально/ віддалено	обмежений	1, 2, 4, 5	user	хмарні/лок альні	корпоратив-ні	є потреба
Відділ продажу							
Керівник	локально/ віддалено	частково обмежений	1, 2, 3, 4, 5	admin/ user	хмарні/лок альні	корпорат/ власні	є потреба
Старший менеджер (2)	локально/ віддалено	обмежений	1, 2, 3, 4, 5	user	хмарні/лок альні	корпорат/ власні	є потреба
Менеджер (5)	локально/ віддалено	обмежений	1, 2, 3, 5	user	хмарні/лок альні	корпорат/ власні	є потреба
Відділ маркетингу							
Керівник	локально/ віддалено	повний	1, 3, 4	admin	хмарні/лок альні	корпорат/ власні	є потреба
Фахівець з реклами (5)	локально/ віддалено	повний	1, 3, 4	admin	хмарні/лок альні	корпорат/ власні	є потреба

Продовження таблиці 3.1.

Посада та кількість співробіт-ників	Режим роботи	Рівень доступу до мережевих ресурсів	Доступ до конфіденці йної інформації	Права в системі	Викорис-товувані сервіси	Робочі пристрої	Необхід-ність виходу в Інтернет
Відділ маркетингу							
Аналітик (2)	локально/ віддалено	повний	1, 3, 4	admin	хмарні/лок альні	корпорат/ власні	є потреба
SMM спеціаліст	віддалено	повний	1, 4, 6	admin	хмарні	влісні	є потреба

Тож організація нараховує 28 співробітників, 3 з яких працюють віддалено, інші у гібридній формі. Всі співробітники мають різні доступи, налаштовані відповідно до визначених груп в AD, до корпоративних ресурсів з корпоративного обладнання, а також мають змогу використовувати власне при віддаленій роботі, підключаючись через VPN. При роботі з корпоративним обладнанням, співробітники мають більшою мірою повний доступ до ресурсів та об’єктів, а також володіють достатньою мірою конфіденційних даних. При використанні власних комп’ютерів, для виконання робочих завдань, співробітники мають повні адміністративні права у своїх облікових записах та є неконтрольованими, оскільки організація не висуває жодних обмежень, щодо використання власних пристроїв. ІТ-відділ та відділ маркетингу мають повні адміністративні права і на корпоративних пристроях, оскільки, цього вимагає специфіка робочих завдань. Відділ маркетингу є творчими підрозділом організації, з постійним та не контрольованим доступом в Інтернет, для пошуку ідей, програм, картинок, музичних плей-листів і т.д. Окрім того Директор організації також не обмежений жодними вимогами. Парольна політика в “Компанія” не є формалізованою та обов’язковою до виконання, співробітники ознайомлені з поняттям інформаційної безпеки на рівні власного сприйняття та розуміння, а також існуючих за змовчуванням обмежень в самих системах, відтак відсутні вимоги щодо довжини та складності пароля, частоти зміни, не використання однакових паролів до різних сервісів та систем, не пересікання паролів від особистих і робочих сервісів та систем.

Спроектована мережа організації (див Рис 3.1, Рис.3.2) має доволі малий розмір та охоплює площу, обмежену одним поверхом будівлі. Вся мережа організації поділена на п’ять підмереж. Функцію маршрутизації та надання доступу до інтернет та підключення до хмарного середовища покладено на Маршрутизатор 1. Перша підмережа (VLAN1) належить IT відділу та складається з 5 робочих станцій (ПК 1-5), сервера (Сервер1), всі хости цієї підмережі об’єднані комутатором (Комутатором 1), який з’єднаний з маршрутизатором мережі (Маршрутизатор 1). Друга підмережа (VLAN2) - це відділ бухгалтерії. Структура цієї підмережі аналогічна попередній і включає в себе 4 робочі станції (ПК 6-9), сервер (Сервер2) та багатофункціональний пристрій (1). Третя підмережа (VLAN3) – група відділу продажу, включає в себе вісім робочих станцій (ПК 10-17) та сервер (Сервер3). Четверта підмережа (VLAN4) – відділу маркетингу, і містить вісім робочих станцій (ПК 28-25), сервер (Сервер4) і багатофункціональний пристрій (2). П’ята підмережа (VLAN5) — у використанні Директора організації та його секретаря, і включає два настільні комп’ютери та багатофункціональний пристрій (2). Хости підмереж 2-5 так само місять об’єднані комутаторами (Комутатор 2-5), які в свою чергу з’єднані з маршрутизатором мережі (Маршрутизатор 1). Окрім того, загальний корпоративний сервер (Сервер 1) має окрему лінію з’єднання з маршрутизатором.

Рис. 3.1. Схема розміщення корпоративних пристроїв у локальній мережі “Компанія”

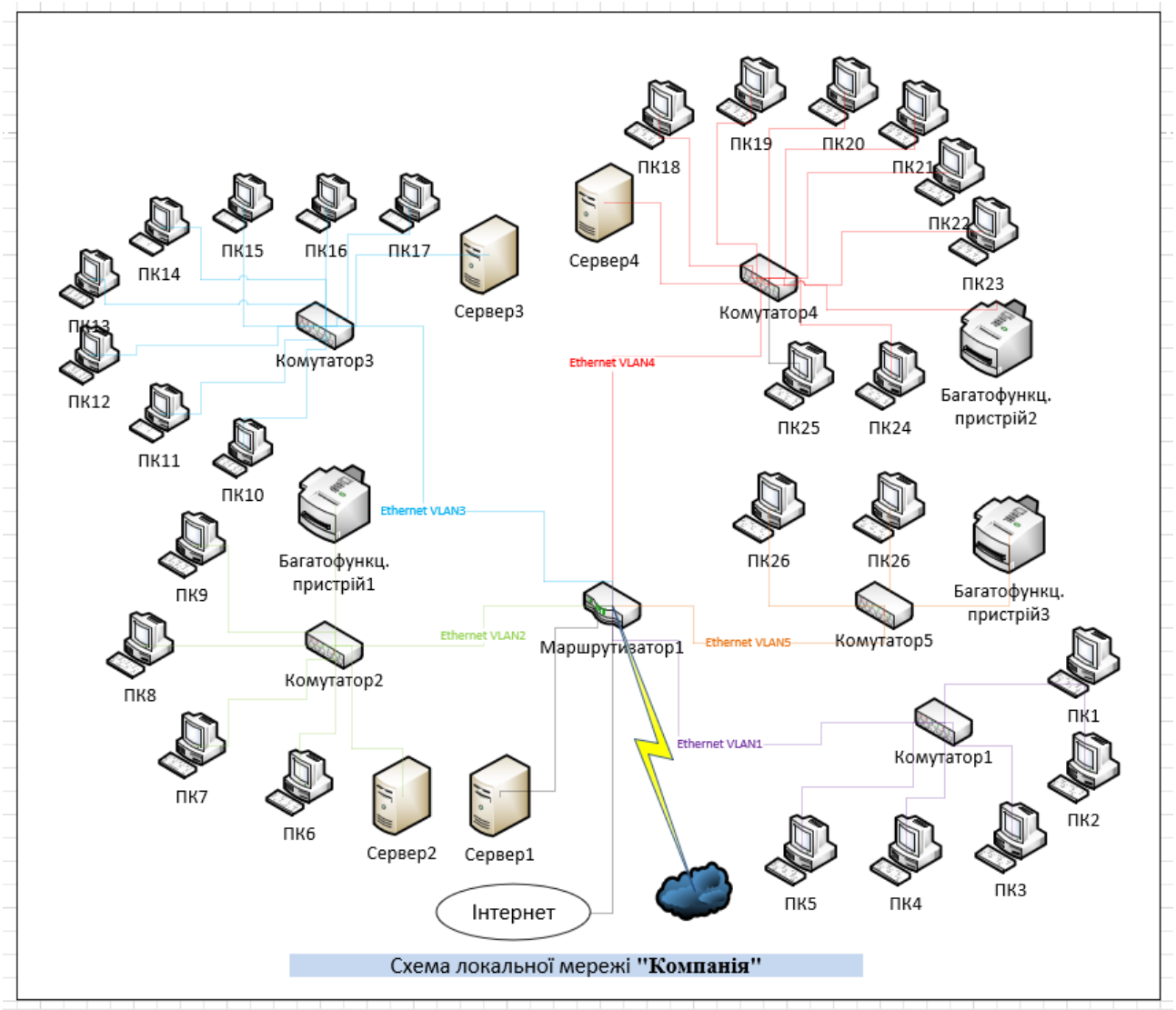

Рис. 3.2. схема локальної мережі “Компанія”

Стосовно корпоративного технічного обладнання: для всіх співробітників в офісі організації встановлені Моноблоки Lenovo ThinkCentre M820z (10SDS05F00) з ОС Windows 10 Pro — 28 шт., багатофункціональні пристрої XEROX WC 3025NI — 3шт., мережеві комутатори D-Link DES-1026G — 5шт., Маршрутизатор D-Link DSR-250, та сервери з встановленою ОС Windows Server 2019. “Компанія” використовує хмарні сервіси Microsoft Office 365 та Azure.

Тож для визначення необхідності для компанії у використанні PAM системи було проведено комплексний аудит (див. Табл.3.2) привілейованих ризиків та прораховано кроки та визначено рішення, які необхідно впровадити, щоб покрити виявлені проблемні зони в політиці безпеки привілейованим доступом (див. Розділ 3.2). У Таблиці позначені узагальнені відповіді більшості

співробітників організації для розуміння потреб, виокремленні і акцентуванні уваги на основних проблемах при забезпеченні привілейованого доступу.

Таблиця 3.2.

Аудит привілейованих ризиків у “Компанія”

Контроль	**Питання аудитора**	**Середньостатистична узагальнена відповідь працівника компанії**
Процес управління привілейованим доступом		
	Чи проваджена в компанії Політика управління привілейованим доступом?	Наявні ручні процеси для управління привілейованим доступом, Політика не формалізована
	Чи мають співробітники права адміністратора на корпоративних комп’ютерах?	Більшість співробітників мають доступ адміністратора на їх робочих та власних машинах.
	Чи наявний впроваджений та контрольований аудит та моніторинг облікових записів привілейованих користувачів?	Перегляд логів можливий та не систематизований, ніхто цим не займається та не контролює
	Чи можуть працівникам надаватись надмірні привілеї?	Якщо адміністратор у системі, то так, контроль за їх діями відсутній Також є практика надання доступів за потреби працівника, але про скасування таких доступів мови не йде, процес не контрольований
	Чи можуть співробітники самі підвищити собі привілеї?	Ті що мають адміністративні права - цілком, якщо знатимуть, як це зробити. В кого обмежені то ні.
	Чи наявні забуті привілейовані облікові записи?	Можуть бути записи колишніх співробітників, реєстру не ведуть
	Чи відслідковуються завантаження програм користувачами з привілейованими правами?	Практика обмеження на відвідування сайтів та встановлення програм присутня, але не всі відділи підпадають під такі обмеження, оскільки цього вимагає робочий процес, наприклад відділ маркетингу
	Чи обмежуються права суперкористувача при використанні Microsoft Office 365?	Хмарне середовище не є сильно контрольованим у цьому плані
	Чи контролюються середовища DevOps?	Середовище розробки розгорнуте в хмарі і не є частиною загальної мережі організації, програміст несе повну відповідальність за все, що там відбувається

Продовження таблиці 3.2.

Контроль	**Питання аудитора**	**Середньостатистична узагальнена відповідь працівника компанії**
Привілейовані парольні дані		
	Чи використовують співробітники унікальні, різносимвольні паролі?	Чітко встановлених вимог нема, тому кожен використовує як бажає, як легше запам'ятати
	Як часто змінюються паролі?	Така практика не встановлена, зміна паролю відбувається за бажанням користувача
	Чи розкривають співробітники свої паролі?	Можуть, якщо існує потреба замінити когось на його робочому місці
	Чи записують співробітники свої паролі на видних місцях чи електронних документах?	Не виключено
Привілейований віддалений доступ		
	Чи може користувач ввімкнути віддалений доступ?	Використовується VPN та RDP протокол для віддаленого доступу до корпоративного віддаленого робочого середовища.
	Чи відслідковується віддалений доступ до мережі компанії?	Детального журналу сеансів не ведеться
	Чи захищаються облікові дані, які використовуються для привілейованого віддаленого доступу?	Практика управління паролями відсутня

Відтак, були визначені наступні критичні точки (див. Табл.3.3) в управлінні привілейованим доступом в "Компанія". Середовище розробки не враховувалось у якості критичної точки, оскільки не входить до загальної мережі компанії, яка розглядається в даній роботі, програміст працює віддалено з використанням хмарних сервісів Azure, які самі забезпечують безпеку своїх хмарних платформ та надають всі інструменти для безпечної розробки.

Таблиця 3.3.

Виявлені критичні точки в управління привілейованим доступом у "Компанія"

Виявлена проблема управління привілейованим доступом в організації	**Опис проблеми**	**Ймовірність загрози-атаки-ризику для організації**
Процес управління привілейованим доступом		

Продовження таблиці 3.3.

Виявлена проблема управління привілейованим доступом в організації	**Опис проблеми**	**Ймовірність загрози-атаки-ризику для організації**
Процес управління привілейованим доступом		
Відсутність формалізованої та впровадженої Політики управління привілейованим доступом	Відсутність обмежень, контролю та забезпечення розподілу і використання прав привілейованого доступу	Несанкціонований доступ до систем та сервісів, інсайдерські атаки
Надмірне надання привілеїв	Кінцеві користувачі рідко скаржаться на надто велику кількість привілей, IT-адміністратори традиційно надають кінцевим користувачам широкі набори привілей	Надлишок привілеїв створює роздуту поверхню атаки. Хакер може використати весь набір привілеїв облікового запису, отримати доступ до даних зараженого комп'ютера та навіть здійснити атаку на інші мережеві комп'ютери чи сервери
Підвищення привілей	Перехід від низького рівня привілейованого доступу до вищого рівня привілейованого доступу	Кібератака з метою отримання незаконного доступу до підвищених прав або привілеїв, що перевищують ті, які має користувач. Передбачає використання вразливості ескалації привілеїв, такої як системна помилка, неправильна конфігурація або невідповідний контроль доступу
Забуті привілейовані облікові записи	Облікові записи можуть нараховуватися у великих кількостях та бути неконтрольованими	Створюють небезпечні бекдори для зловмисників, зокрема колишніх співробітників, які залишили компанію, але зберегли доступ
Відсутність належного аудиту та моніторингу дій привілейованого користувача	Неможливо прив'язати дії, які виконуються з обліковим записом, до однієї особи. Це створює проблеми з безпекою, неможливістю перевірки та відповідністю.	Один зламаний обліковий запис може поставити під загрозу безпеку інших облікових записів
Надмірні привілеї для встановлення та запуску програм	Користувачі можуть без особливих зусиль запускати програми від імені адміністратора і керувати ними	Неправильна конфігурація, уразливості і експлойти, а також цілеспрямовані інсайдерські атаки.

Продовження таблиці 3.3.

Виявлена проблема управління привілейованим доступом в організації	Опис проблеми	Ймовірність загрози-атаки-ризику для організації
Привілейовані парольні дані		
Співробітники схильні забувати паролі	Велику кількість (постійно змінних) паролів, застосовування однакових паролів для кількох облікових записів, паролі які легко вгадати	Зловмисники можуть використовувати автоматичні зломщики паролів, щоб вгадати паролі за замовчуванням. Поверхня атаки, яку це представляє, може бути великою, якщо однакові параметри за замовчуванням використовуються на багатьох різних кінцевих точках
Спільний доступ до пароля	Розкриття паролів, запис паролів на папері чи в електронних документах, таких як MS Word або електронних таблицях	Хакери можуть співвіднести, разом із адресами електронної пошти та іменами користувачів, пароль від одного зламаного облікового запису до інших служб або облікових записів, які можуть використовувати той самий пароль
Привілейований віддалений доступ		
Відсутність належного аудиту та моніторингу дій привілейованого користувача при віддаленому доступі	Неможливо переконатись що авторизація, надана за допомогою віддаленого доступу або третій стороні, використовується належним чином	Бекдори для проникнення хакерів на критично важливі сервери, перехоплення привілейованих автентифікаційних даних

Тож, чим більше привілеїв і доступів отримує користувач, обліковий запис або процес, тим більший потенціал для зловживань, використання чи помилок.

3.2. Технологія управління привілейованим доступом на базі рішень BeyondTrust Privilege Management для покриття визначених критичних точок у корпоративній інформаційній системі

Провівши аудит привілейованого доступу в організації та визначивши

критичні точки та область, доцільно наголосити на наступному:

- співробітники компанії значну частину часу працюють **віддалено**;
- для виконання своїх посадових обов'язків, працівники використовують **хмарні сервіси** такі як Microsoft Office 365;
- рутинна робота на корпоративному ПК може передбачати використання **облікового запису користувача з** визначеними у ньому **правами адміністратора** для перегляду Інтернету, відео, скачування та запуску програм і сервісів необхідних для роботи, з невідомих джерел.

Відтак, основні зони, до яких була прикута увага при проведенні аудиту, визначили необхідність контролювати привілейований доступ співробітників організації, з огляду на виробничу необхідність працівників мати привілейовані облікові записи. Так, при підборі рішень для реалізації управління привілейованим доступом, у якості рекомендованих для подальшого впровадження були обрані рішення від BeyondTrust Privilege Management, що засновані на оцінці ризиків та потребах організації. Рішення були обрані з огляду на бізнес-потреби в організації та для захисту: привілейованих облікових записів та їх привілейованих даних, віддаленого доступу, доступу та роботи з хмарними сервісами (див. Табл.3.4).

Таблиця 3.4.

Рішення BeyondTrust Privilege Management для покриття виявлених критичних точок у "Компанія"

Рішення від BeyondTrust Privilege Management для покриття виялених проблемних областей	**Виявлена проблемна область**	**Опис рішення**
Cloud Vault	Управління привілейованим доступом	Являє собою хмарне сховище для зберігання привілейованих облікових записів
Password Safe	Привілейовані парольні дані	Об'єднує привілейований пароль і керування привілейованим сеансом, надаючи комплексне виявлення, керування, аудит і моніторинг для будь-якого привілейованого облікового запису чи даних об'єкта.

Продовження таблиці 3.4.

Рішення від BeyondTrust Privilege Management для покриття виялених проблемних областей	**Виявлена проблемна область**	**Опис рішення**
Privilege Remote Access	Привілейований віддалений доступ	Дозволяє контролювати доступ співробітників, вендорів, служб підтримки з використанням принципу найменших привілей. Рішення надає можливість здійснювати віддалений доступ та використовує сховище паролів для виявлення та управління привілейованими обліковими даними.

В результаті впровадження “Компанія” може отримати:

- Password Safe та BeyondTrust Privileged Remote Access, які забезпечать безпечний віддалений доступ за допомогою єдиного підходу до забезпечення безпеки підключення та автоматичної перевірки привілейованих облікових даних та повного запису сеансу доступу.
- Інтеграцію Cloud Vault з Privileged Remote Access, яка усуне необхідність запам’ятовувати паролі та логіни кінцевим користувачам та зберігає записи журналів для кожного віддаленого сеансу.

Таким чином, при впровадженні даних рішень, відбувається покриття всіх попередньо визначених критичних точок, а саме: надмірне надання привілей, неконтрольоване підвищення привілей, відсутність належного аудиту та моніторингу дій привілейованого користувача, людський фактор, віддалений доступ.

Тож, у процесі впровадження попередньо визначених рішень від BeyondTrust Privilege Management “Компанія” може розглянути та провести наступні налаштування для забезпечення управління привілейованим доступом та підвищення рівня захисту, а також відповідності стандартам безпеки:

1) Password Safe працює з керованими системами з якими взаємодіє обліковий запис. Адміністратор можете переглядати відомості про керовану систему (див. Рис.3.3, Рис.3.4), такі як:

- Визначення деталей, атрибутів і політик;

- Керовані облікові записи в керованій системі;
- Розумні групи, пов’язані з керованою системою;
- Облікові записи, пов’язані з керованими обліковими записами в керованій системі;
- Відкриті ключі, пов’язані з керованою системою;
- Функціональний обліковий запис для керованої системи;

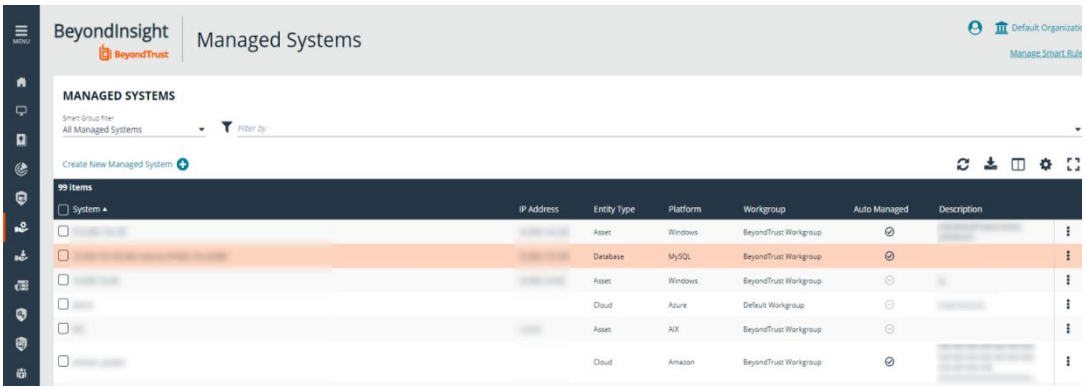

Рис. 3.3.Панель управління керованими системами в Password Safe

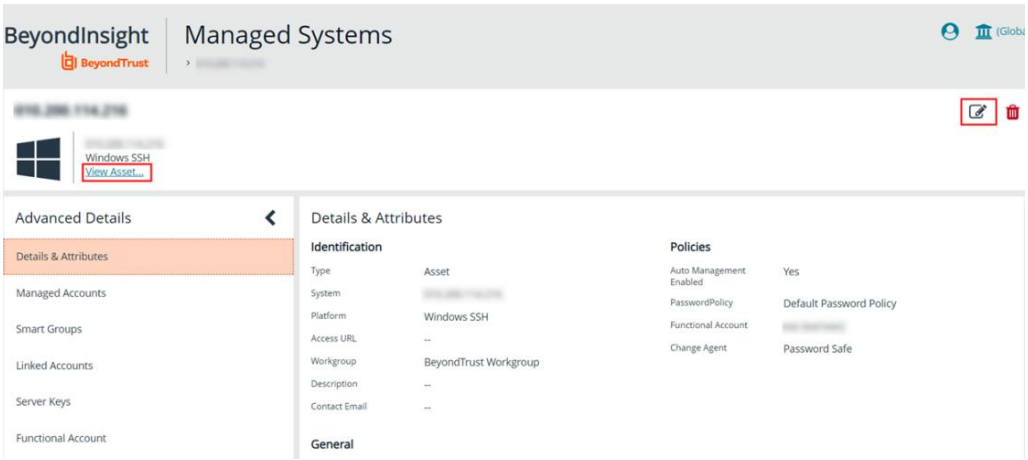

Рис. 3 4. Пов’язані деталі та атрибути з керованими системами

Керовані облікові записи – це облікові записи користувачів, які є локальними або обліковими записами активного каталогу в керованій системі.

Після того, як обліковий запис буде додано до керування Password Safe (див. Рис.3.4), адміністратор даної системи може:

- Переглядати атрибути та налаштування, призначені обліковому запису, наприклад його ідентифікаційні дані, налаштування та політики.
- Переглядати керовані системи, пов’язаних з обліковим записом.

- Переглядати смарт-групи, пов’язані з обліковим записом, а також дату останньої обробки та статус обробки.
- Переглядати, які облікові записи синхронізовано з керованим обліковим записом.
- Переглядати список змінених паролів і причину кожної зміни.

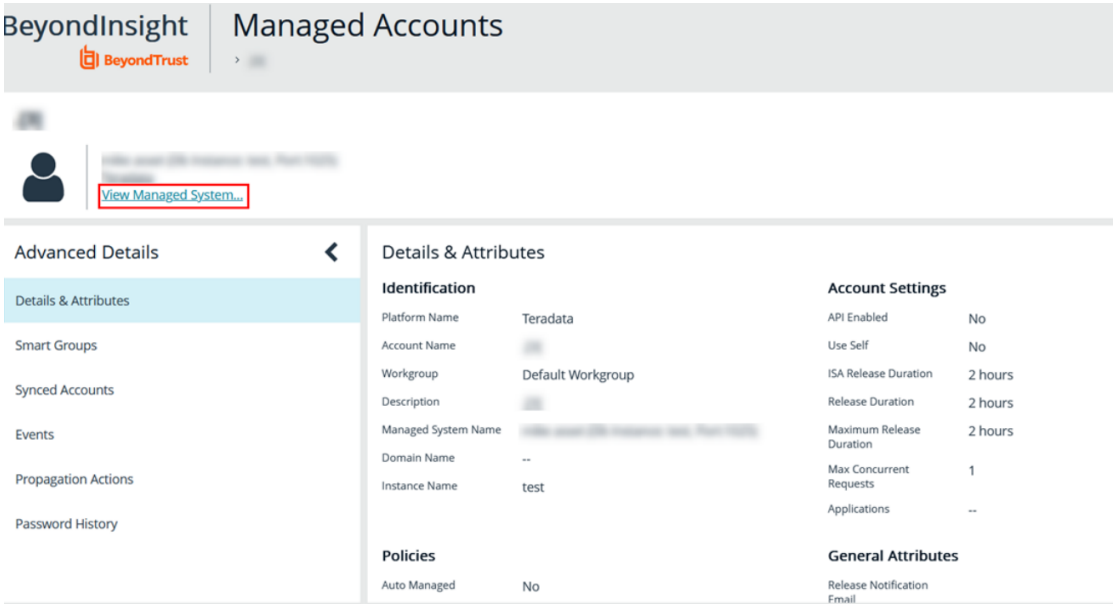

Рис. 3.4. Панель управління керованими обліковими записами в Password Safe

Такий підхід дозволить вирішити визначену проблему, пов’язану з відсутністю належного аудиту та моніторингом дій привілейованих користувачів. Використання такого функціоналу створює можливість контролю користувачів та їх доступів до програм, і сервісів, які вони використовують залежно від групи користувача та призначеної ролі.

Для створення груп користувачів та призначення їм ролей Password Safe визначає наступну послідовність дій:

- На лівій панелі навігації в консолі обрати Конфігурація.
- У розділі «Доступ на основі ролей» обрати «Керування користувачами».
- Натиснути “Створити нову групу”.
- Обрати “Створити нову групу”.

- Ввести назву та опис групи.
- Натиснути “Створити групу”.
- Призначити користувачів до групи:
  – У розділі «Відомості про групу» обрати «Користувачі».
  – У розкривному списку «Показати» обрати «Непризначені користувачі».
  – Вибрати користувачів, яких потрібно додати до групи, а потім натиснути “Призначити користувача” (див. Рис 3.5).

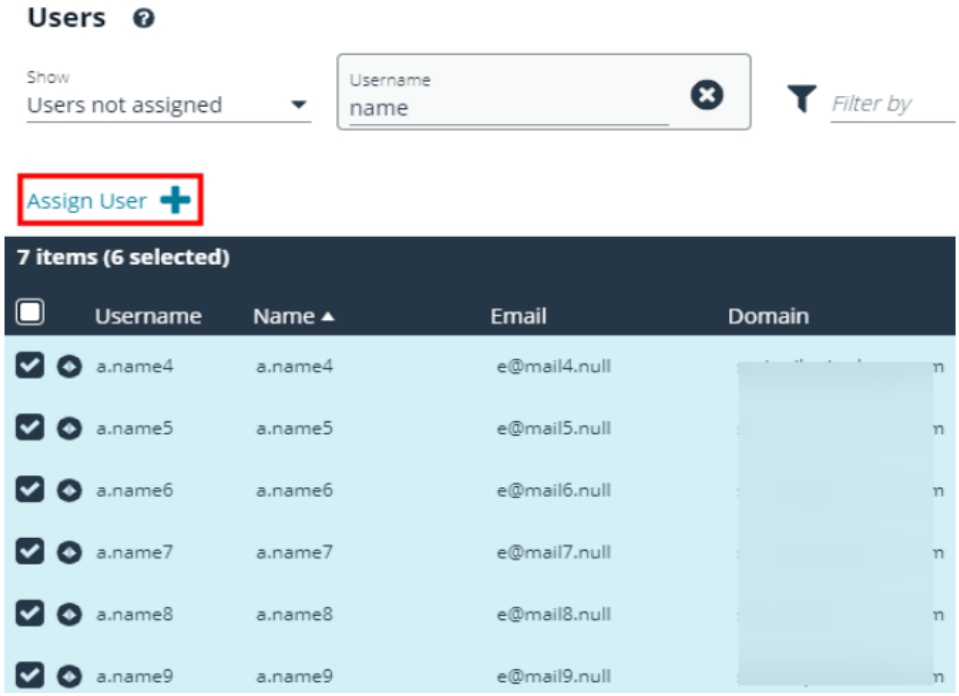

Рис. 3.5. Вибір користувачів для додавання до групи

- Призначити групі дозволи на функції:
  – У розділі «Відомості про групу» обрати «Функції».
  – Обрати функції, яким потрібно призначити дозволи, а потім натиснути «Призначити дозволи».
  – Обрати «Призначити дозволи лише для читання» або «Призначити повний контроль дозволів».
- Призначити групі дозволи та ролі Smart Groups:
  – У розділі «Відомості про групу» обрати «Розумні групи».

– Вибрати смарт-групу чи групи, яким потрібно призначити дозволи, а потім натиснути «Призначити дозволи».

– Вибоати «Призначити дозволи лише для читання» або «Призначити повний контроль дозволів».

– Вибрати інтелектуальну групу, якій потрібно призначити Password Safe ролі, а потім натиснути кнопку “Додаткові параметри”.

– Дибрати “Редагувати ролі Password Safe” (див. Рис.3.6).

– Вибрати роль(і).

– Клацнути «Зберегти ролі».

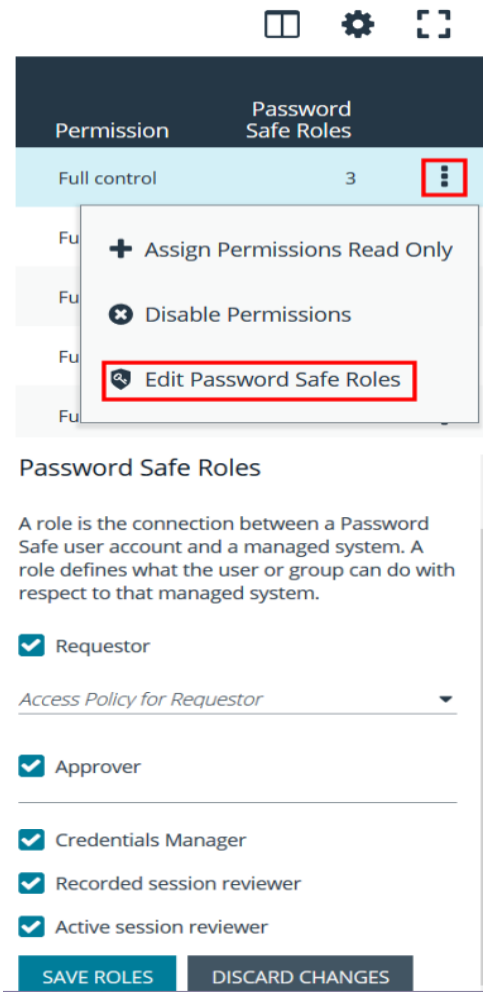

Рис. 3.6. Редагування ролей Password Safe

Після проведення таких налаштувань, можна вирішити проблему, пов’язану з надмірним наданням привілей оскільки доступи для співробітників для виконання тих чи інших функцій у системі відтепер контролюватимуться та

надаватимуться за принципом найменших привілей і лише для виконання необхідних завдань.

Також, існує можливість реалізувати контроль за користувачами, що захочуть здійснити вхід у систему Password Safe для підвищення власних привілей. Можна вимкнути прямий доступ до URL-адреси веб-порталу Password Safe і тоді користувачі повинні будуть надавати SAML, смарт-картку або облікові дані з підтримкою претензій, перш ніж отримати доступ до веб-порталу. Налаштування можна застосувати до локальних користувачів:

- На лівій панелі навігації в консолі обрати Конфігурація.
- У розділі «Доступ на основі ролей» обрати «Керування користувачами».
- Натиснути Користувачі, щоб відобразити список користувачів у сітці.
- Вибрати користувача, а потім натисніть кнопку “Додаткові параметри”.
- Вибрати “Редагувати дані користувача”.
- Натиснути перемикач, щоб змінити параметр «Вимкнути форми входу» на «так» (див. Рис.3.7).

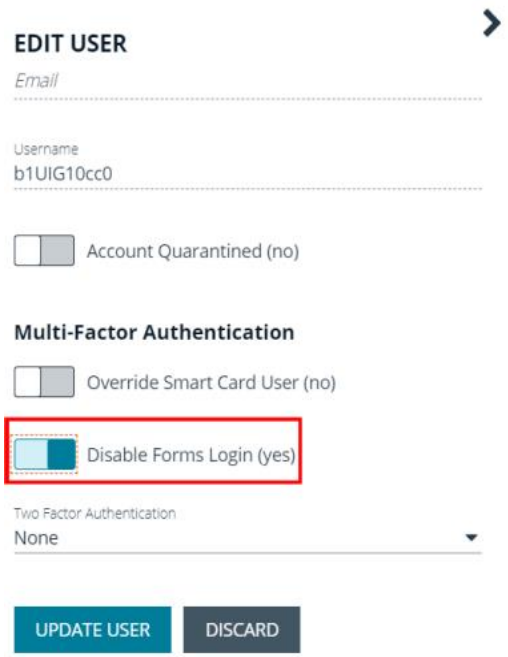

Рис. 3.7. Редагування даних користувача

Дане налаштування усуває можливості навіть привілейованим користувачам підвищувати собі привілеї, що покриває ще одну, з визначених у процесі аудиту, критичну точку.

Password Safe поставляється з політикою паролів за замовчуванням, яка використовується для створення нових паролів для автоматично керованих облікових записів. Можна змінити налаштування для політик за замовчуванням, наприклад довжину та складність пароля. Також можна створити нову парольну політику (див. Рис.3.8):

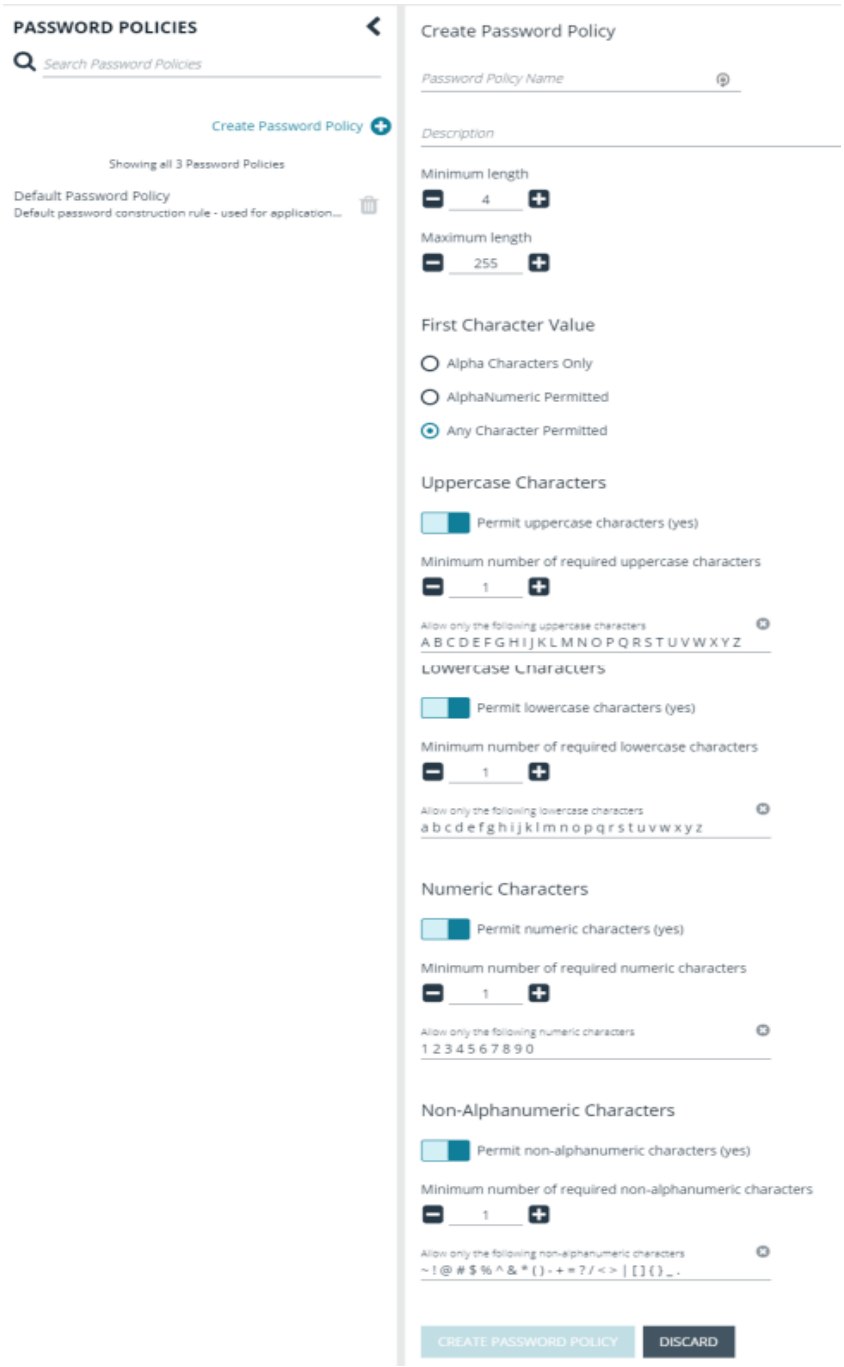

Рис. 3.8. Налаштування парольних політик

- У консолі BeyondInsight перейти до “Конфігурація” > “Привілейовані Політики керування доступом” > “Політики паролів”.
- Натиснути “Створити політику паролів”.
- Ввести назву та опис політики паролів.
- Установити наступні параметри для своєї політики:
  - Мінімальна та максимальна кількість символів;
  - Значення першого символу;
  - Великі символи;
  - Символи нижнього регістру;
  - Цифрові символи;
  - Не буквено-цифрові символи;
  - Мінімальна кількість символів, які не є алфавітно-цифровими.
- Після завершення натисніть «Створити політику паролів».

Дані можливості покривають виявлені проблеми у “Компанія” з відсутністю парольної політики та вимог до неї.

Також, для контролю доступів до програм, до Password Safe можна додати перелік програм та визначити запити для запуску сеансів, їх запису. Щоб додати програму до керування Password Safe, потрібно виконати такі дії:

- Налаштувати деталі програми в конфігурації Password Safe.
- Пов’язати програму з керованим обліковим записом.
- Створити політику доступу, яка дозволяє програмі доступ. Тут можна ввімкнути запис і журнал натискань клавіш.
- Створити групу користувачів, яка включає керовані облікові записи.
- Призначити роль запитувача (або роль запитувача), яка включає вибір політики доступу.

Таким чином вирішується проблема, пов’язана з надмірними привілеями для встановлення та запуску програм, оскільки відтепер всі дії є контрольованими та підлягають моніторингу.

2) Remote Access можна використовувати для прозорої роботи через

брандмауери, забезпечуючи з'єднання з будь-яким комп'ютером із підключенням до Інтернету в будь-якій точці світу. Однак потрібна певна конфігурація (див. Рис.3.9).

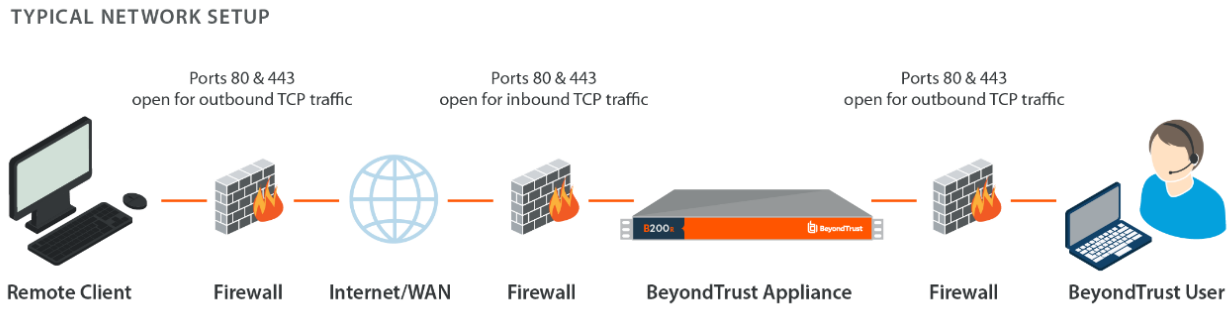

Рис. 3.9. Конфігурація Remote Access

Порти 80 і 443 мають бути відкриті для вихідного трафіку TCP на брандмауерах віддаленої системи та локального користувача. На Рис. Показана типова конфігурація мережі.

Пристрій BeyondTrust Appliance служить центральною точкою адміністрування та управління віддаленим доступом, а також підтримує протокол керування мережею (SNMP). Це дозволяє інструментам, які збирають доступність та іншу статистику через протокол SNMP, надсилати запити до пристрою для досягнення цілей моніторингу. Щоб увімкнути SNMP для цього пристрою, потрібно (див. Рис.3.10):

- Встановити прапорець «Увімкнути SNMPv2» або «Увімкнути SNMPv3». Це дозволяє серверу SNMPv2 або v3 відповідати на запити SNMP.
- Ввести значення для назви групи лише для читання, розташування системи та обмежень IP для IP-адрес, яким дозволено надсилати запити цьому пристрою за допомогою SNMP. Якщо в полі IP Restrictions не введено жодної IP-адреси, доступ надається всім хостам.
- Якщо вибрано SNMPv3:
  - Ввести ім'я користувача та пароль.
  - Вибрати спосіб автентифікації зі спадного меню.
  - Поставити прапорець SNMPv3 Enable Privacy, якщо потрібно

шифрувати зв’язок.

– Ввести пароль конфіденційності та виберіть метод конфіденційності.

- Після завершення натисніть «Зберегти зміни».

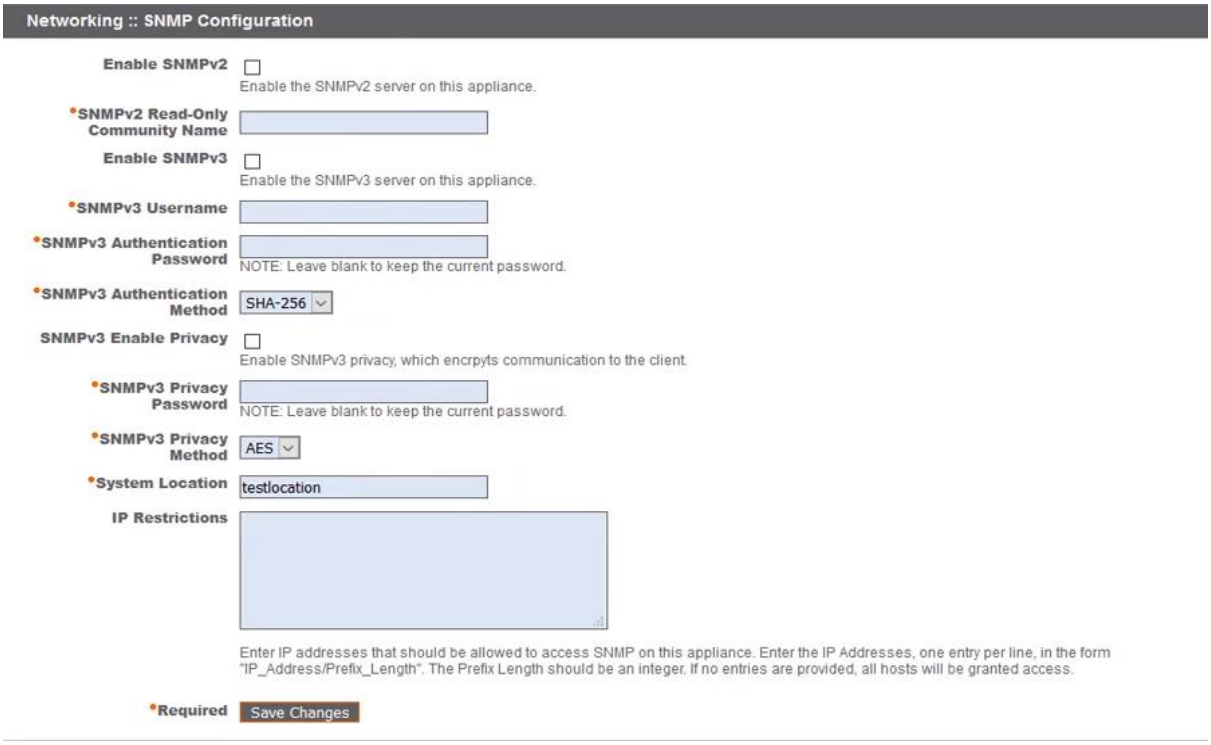

Рис. 3.10. SNMP конфігурація

Також надає можливість реєстрації сеансів, де усім сеансам призначається унікальний ідентифікатор сеансу, який називається LSID — це рядок із 32 символів, який є унікальним для кожного сеансу. Окрім того існує можливість увімкнення запису відеосесії. Для налаштування сеансів, потрібно визначити їх параметри:

- Параметри сеансу: Вимагати закритих сеансів після виходу з системи або виходу. Якщо встановити прапорець «Вимагати закритих сеансів під час виходу» або «Вийти», користувачі не зможуть вийти з консолі, якщо матимуть відкриті вкладки сеансу.
- Параметри підключення: Час очікування повторного підключення: визначити, як довго відключений клієнт кінцевої точки може намагатися повторно підключитися. Обмежити фізичний доступ до кінцевої точки, якщо

кінцева точка втрачає з’єднання або якщо сеанс відключено для всіх користувачів.Якщо з’єднання сеансу втрачено, введення миші та клавіатури віддаленої системи можна тимчасово вимкнути, відновивши або коли підключення відновлюється або коли сеанс припиняється.

- Доступ до параметрів реєстрації сеансу: Увімкнути запис спільного доступу до екрана: вибрати, чи сеанси показу екрана повинні автоматично записуватися як відео. Встановити роздільну здатність для перегляду відтворення запису сеансу. Увімкнути запис користувача.Встановити роздільну здатність для перегляду відтворення запису сеансу.
- Вибрати, чи повинні користувачі отримувати підказку про те, що їх робочий стіл буде записано.

Серед всього функціоналу BeyondTrust Appliance надає змогу керувати користувачами (див. Рис.3.11), додавати їх (див. Рис.3.12), видаляти та змінювати паролі.

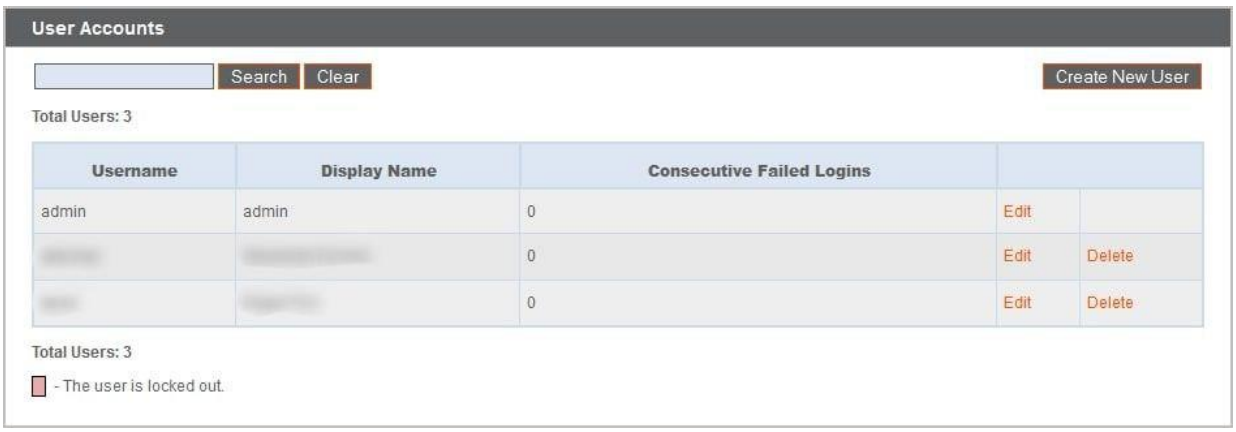

Рис. 3.11. Управління користувачами за допомогою BeyondTrust Appliance

Рис. 3.12. Додавання нового користувача за допомогою BeyondTrust Appliance

Таким чином вирішується проблема, пов’язана з відсутністю належного аудиту та моніторингу дій привілейованого користувача при віддаленому доступі, оскільки Remote Access зберігає записи журналів для кожного віддаленого сеансу.

3) BeyondTrust Vault — це сховище облікових даних, яке існує на пристрої BeyondTrust Appliance. Vault зберігає дані в базі даних у зашифрованому форматі. Паролі та приватні ключі SSH шифруються в стані спокою за допомогою AES-256-GCM на додаток до будь-якого повного дискового шифрування, увімкненого для пристрої.

Рішення дозволяє переглядати кінцеві точки, пов’язані з обліковим записом та обирати користувачів, яким дозволено доступ. Інформація про облікові записи включає:

- Тип облікового запису, зокрема доменний чи локальний, або обліковий запис із загальним паролем.
- Ім'я облікового запису.
- Ім’я користувача, пов’язане з обліковим записом.
- Групу облікових записів, до якої належить обліковий запис.
- Кінцева точка, з якою пов’язаний обліковий запис.
- Політика облікового запису яку використовує обліковий запис Vault.
- Опис облікового запису.
- Останню перевірку облікового запису.
- Вік пароля
- Статус облікового запису.

Vault покриває проблему запам’ятовування надмірної кількості паролів для доступу до необхідних служб та сервісів, оскільки користувачі можуть просто вибрати правильні облікові дані зі спадного списку та увійти безпосередньо у віддалену систему, навіть не знаючи чи переглядаючи справжній пароль.

Отже, скориставшись даними рішеннями та базовими налаштуваннями, “Компанія” покриє всі попередньо визначені критичні точки в управлінні

привілейованим доступом, забезпечуючи функціонування парольної політики, а також покращуючи надійність та умови реалізації віддаленої роботи, здійснюючи її контроль та моніторинг.

3.3. Розробка рекомендацій щодо застосування технології управління привілейованим доступом корпоративної інформаційної системи на базі рішень BeyondTrust Privilege Management

Провівши попередній аудит привілейованого доступу, визначивши критичні точки, та здійснивши їх покриття рішеннями BeyondTrust Privilege Management, доцільно надати кілька ключових рекомендацій щодо управління привілейованим доступом в організації:

1. Контроль і аудит над привілейованими ідентифікаторами та діями для захисту корпоративних активів і користувачів у світі без периметра та роботи з будь-якого місця, беззаперечно велика перевага, особливо при забезпеченні відповідності стандартам з інформаційної безпеки. Тому мають бути визначені всі користувачі мережі, особливо привілейовані, їх групи та призначені їм відповідні ролі.
2. Найкращою практикою залишається використання привілейованих облікових записів адміністраторів лише за крайньої необхідності та протягом обмеженого необхідного часу. Звичайні облікові записи не мають використовуватись для вирішення адміністративних завдань при використанні гібридного середовища, як це реалізовано у «Компанія». Тому при налаштуванні параметрів сесій не варто забувати про дані обмеження та не нехтувати ними.
3. Привілейованим записам повинні бути призначені лише ті програми, які їм потрібні для виконання адміністративних завдань. Дане налаштування можна реалізувати у Password Safe, як це було описано у попередніх пунктах. Таким чином, порушення безпеки у хмарному середовищі не вплинуть на локальне, та навпаки.
4. У подальшому, з огляду на фінансові можливості організації та за

необхідності, варто розглянути рішення DevOps Secret Safe для забезпечення контрольованої безпеки у хмарному середовищі розробки. Хоча “Компанія” впевнена у відповідальному ставленні програміста до безпеки розробки, все ж поняття ІБ та безпека ІТ дещо різняться у сприйнятті. Оскільки в загальному розумінні безпека сайту з точки зору програміста — це забезпечення його доступності. ІБ ж розглядає різні аспекти, включаючи: безпечне середовище для розробки, відокремлені середовища для розробки, тестувань та впровадження, а також унеможливлення використання критичних даних організації в попередніх процесах.

5. Окрім того, організація може цілком відмовитись від використання VPN, яка надає велику кількість доступів і не має достатнього контролю для привілейованих випадків використання, тому що запропоновані рішення BeyondTrust Privilege Management спрощують віддалений доступ і забезпечують дотримання найкращих практик управління привілеями, таких як: найменші привілеї, нульова довіра.

6. Загалом рішення управління привілейованим доступом BeyondTrust надають безліч можливостей для реалізації всіх амбіцій в управлінні привілейованим доступом, а також: підтримку і розширену документацію.

ВИСНОВКИ

Privileged Access Management є найкращим рішенням для зменшення ризиків, що пов’язані з використанням привілейованих облікових записів. PAM корпоративного рівня гарантують, що співробітники мають лише системні привілеї, права та дозволи, необхідні їм для виконання своєї роботи. Таким чином забезпечується найвищий рівень захисту складних розподілених середовищ, а привілейований доступ отримує найвищий пріоритет у забезпеченні безпеки.

1. Тож в даній роботу було виконано наступні завдання:

- досліджено сутність проблеми управління привілейованим доступом корпоративної інформаційної системи;
- встановлено сутність завдань з управління привілейованим доступом;
- проаналізовано існуючі технології, визначено методи та засоби управління привілейованим доступом на основі класу рішень BeyondTrust Privilege Management.;
- проаналізовано основні функції та принципи реалізації управління привілейованим доступом на підприємстві на базі класу рішень BeyondTrust Privilege Management..

2. На основі проведеного аналізу, в роботі було:

- встановлено зміст проблеми, визначено мету та завдання управління привілейованим доступом корпоративної інформаційної системи;
- змодельовано топологію, визначено та покрито критичні точки в управлінні привілейованим доступом в організації на базі рішень BeyondTrust Privilege Management;
- розроблено рекомендації щодо застосування технології з управління привілейованим доступом на підприємстві.

Відтак скориставшись рішеннями BeyondTrust Privilege Management організація може повноцінно забезпечити контроль та моніторинг привілейованого доступу, а також управління ним, з дотриманням найкращих практик та відповідностей міжнародним стандартам.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is Privileged Access Management? [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam
2. What Is Least Privilege & Why Do You Need It? [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/blog/entry/what-is-least-privilege
3. OWASP Top Ten [Електроний ресурс] – Режим доступу: https://owasp.org/www-project-top-ten/. – 13.09.2022 р.
4. Контроль привілейованих користувачів. Що таке PAM-система? [Електроний ресурс] – Режим доступу: https://www.it-world.ru/cionews/security/147451.html – 01.08.2019р.
5. 2021 IBM Security X-Force Insider Threat Report. [Електроний ресурс] – Режим доступу: https://www.ibm.com/downloads/cas/YNAPDA6B. – 14.09.2022 р.
6. Державна служба спеціального зв'язку та захисту інформації України. [Електроний ресурс] – Режим доступу: https://instagram.com/dsszzi?utm_medium=copy_link. – 14.09.2022р.
7. Привілейований доступ: стратегія [Електроний ресурс] – Режим доступу: https://docs.microsoft.com/ru-ru/security/compass/privileged-access-strategy – 03.09.2022 р.
8. Privileged Access Management. [Електроний ресурс] – Режим доступу: https://oneidentity.bakotech.com/privileged-access-management. – 19.09.2022 р.
9. Privileged Access Manager (Pam). [Електроний Ресурс] – Режим Доступу: Https://Softprom.Com/Ru/Vendor/Cyberark/Product/Pam – 19.09.2022 Р
10. Superuser/Superuser Accounts [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/resources/glossary/superuser-superuser-accounts
11. Privileged Password Management [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/resources/glossary/privileged-password-management
12. Secrets Management [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/resources/glossary/secrets-management
13. Privilege Escalation Attack and Defense Explained [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained
14. Privileged Remote Access [Електроний ресурс] – Режим доступу: https://www.beyondtrust.com/remote-access
15. The Cost of Insider Threats 2020. [Електроний ресурс] – Режим доступу: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/ – 14.09.2022 р
16. Практика використання, нові функції і сценарії роботи PAM. [Електроний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/PAM-using-new-Features-and-Scenarios#part3. – 09.02.2022р.
17. Privileged Access Management: Essential and Advanced Practices. [Електроний ресурс] – Режим доступу: https://www.ekransystem.com/en/blog/pam_best_practices. – 27.04.2022 р.
18. Privileged Access Management Solutions Market. [Електроний ресурс] – Режим

доступу: https://www.alliedmarketresearch.com/privileged-access-management-solutions-market-A12403. – 13.07.2021 р.
19. PAM in the cloud vs. PAM for the cloud. What's the difference?. [Електроний ресурс] – Режим доступу: https://delinea.com/blog/pam-privileged-access-management-in-vs-for-the-cloud. – 20.09.2022 р.
20. PAM – управління привілейованим доступом [Електроний ресурс] – Режим доступу: https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions/
21. What Is Privileged Access Management (PAM)? [Електроний ресурс] – Режим доступу: https://heimdalsecurity.com/blog/privileged-access-management-pam/
22. What Are The Best Practices For A PAM Solution And Privileged Access Management? [Електроний ресурс] – Режим доступу: https://www.brainwavegrc.com/privileged_access_management_best_practices/
23. Buyer's Guide for Complete Privileged Access Management [Електроний ресурс] – Режим доступу: file:///C:/Users/USER/OneDrive/%D0%A0%D0%BE%D0%B1%D0%BE%D1%87%D0%B8%D0%B9%20%D1%81%D1%82%D1%96%D0%BB/BeyondTrust_PAM-Buyers-Guide_2022.pdf
24. Інструмент організації технічної підтримки віддалених користувачів BeyondTrust Remote Support, одне з рішень платформи універсального управління привілеями BeyondTrust [Електроний ресурс] – Режим доступу: beyondtrust_remote_support_instrument_organizacii_tehnicheskoj_podderzhki_udalennyh_polzovatelej.pdf
25. The Guide To Multicloud Privilege Management [Електроний ресурс] – Режим доступу: https://assets.beyondtrust.com/assets/documentsBT_WhitePaper_TheGuidetoMulticloudPrivilegeManagement.pdf
26. BeyondTrust Universal Privilege Management [Електроний ресурс] – Режим доступу: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:BeyondTrust_Universal_Privilege_Management
27. Універсальне управління привілеями в компанї [Електроний ресурс] – Режим доступу: beyoundtrust_universalnoe_upravlenie_privilegiyami_v_kompanii.pdf
28. ////

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ