

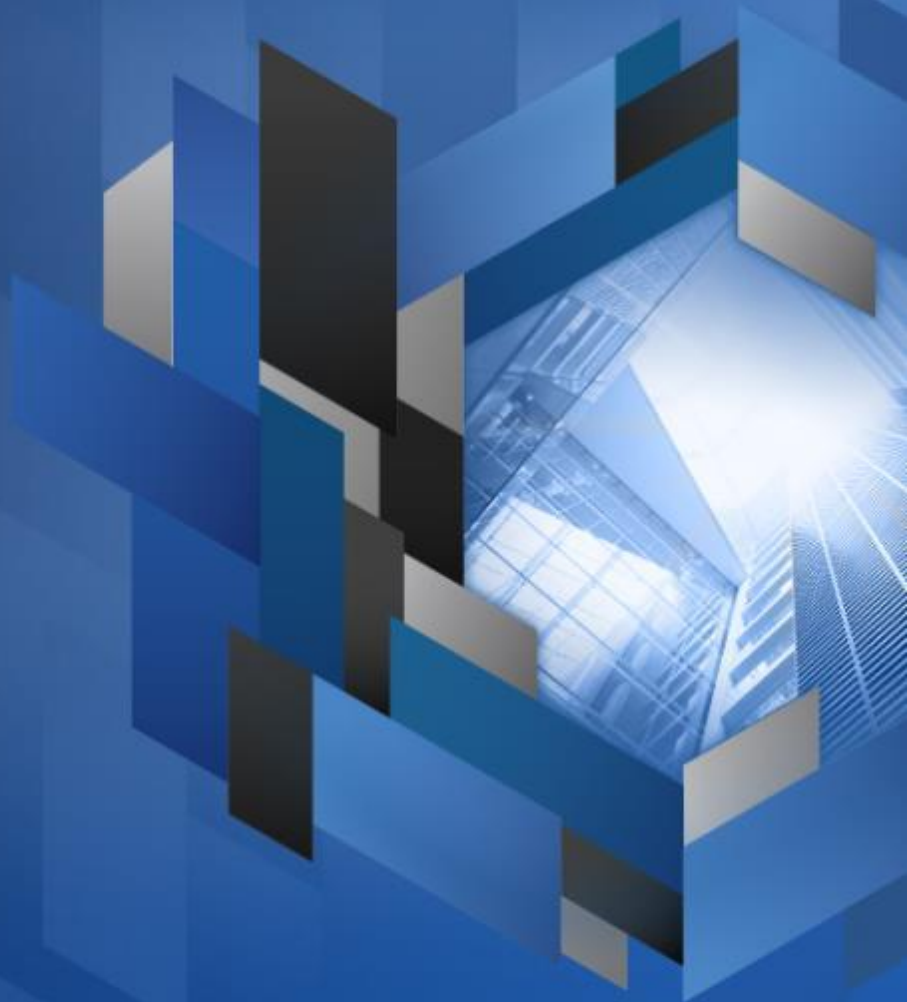


CYBERARK

Решения для телекома

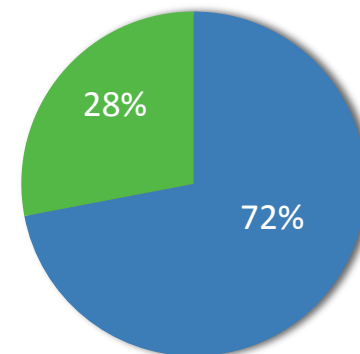
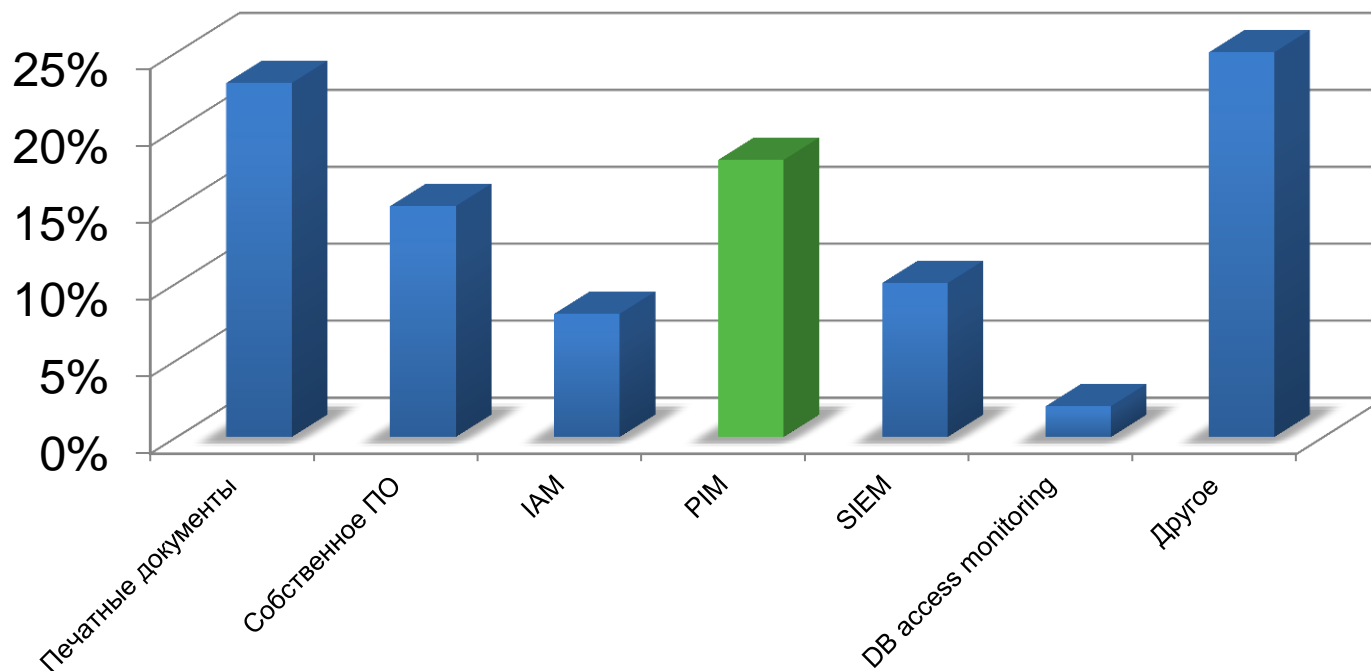
Богдан Тоболь

Региональный директор по продажам



Используются вариации разных решений

Как вы отслеживаете активность привилегированных записей?



Вы отслеживаете привилегированную активность?

Мониторинг и запись привилегированной активности



Установить единую точку управления привилегированными сессиями



Изолировать вредоносный код от целевых систем



Отслеживать и записывать активность на уровне команд



Выбрать масштабируемую архитектуру, не влияющую на инфраструктуру и бизнес



PSM - контроль привилегированных сессий



- Контролирует кто может подключаться к привилегированной сессии и как долго

- Г
- П
- С
- В
- Д

SO без пересылки

Request Details

Status: Request is waiting: 1 more user(s)

Requested on: 3/1/2011 10:21:45 AM

Requestor: John

Operation: Retrieve password PCI DSS Window

Safe name: Domain Admin Accounts (PSHRemoteMachine=Component)

Reason: Make a Configuration Change

Access Type: Multiple operations from 3/1/2011

Emergency: Yes

Reference No: 1892

Authorization required from

- Administrator
- N/A (Vault Administrators)

Authorize Access

Reason:

Confirm Reject

Password

Task Manager

Task Manager

Services MMC

Command Line

Connect

Copy Shortcut

Name: Administrator23

Last verified: N/A

Last modified: Administrator (11/17/2010 12:40:14 PM)

Last used: Administrator (11/17/2010 12:40:14 PM)

User Name: Administrator

Address: Server1

PSM – мониторинг в реальном времени

Monitor

The screenshot displays the CyberArk Privileged Identity Management (PSM) interface. At the top, the title bar reads "Cyber-Ark Privileged Identity Management" with a date of "26/01/2012" and navigation links for "About", "Logout mike", and "Help". Below the title bar, there is a "Sessions" dropdown menu and a "Customize" button. The main area is titled "Search for Sessions" and contains search filters for sessions, commands, and events, along with radio buttons for "Search for recordings" (selected) and "Search for live sessions". A "Search" button is present. On the left, a "Views" sidebar shows "Sessions View" and "Live Sessions" selected. The central table, titled "Live Sessions", lists active sessions with columns for User, From IP, Client, Account User Name, Account Address, Account Policy ID, and Start. Two sessions are listed: one for user "mike" (test_admin) and another for "mike" (Administrator). A red circle highlights a "Terminate" button next to the second session. The bottom of the interface shows a footer with "Copyright © 1999-2012 Cyber-Ark® Software, Ltd. All Rights Reserved.", a "Done" button, and system status information including "Internet | Protected Mode: On" and a zoom level of "125%".

User	From IP	Client	Account User Name	Account Address	Account Policy ID	Start	
mike	192.168.47.148	RDP	test_admin	1.1.1.3	WinDomain	26/01/2012 15:04:55	
mike	192.168.47.148	RDP	Administrator	1.1.1.4	WinDomain	26/01/2012 15:04:55	Terminate



CYBERARK®

PSM – мониторинг аккаутов



- Видеозапись
- Запись текста
- Аудит по...
- М...

The screenshot displays the CyberArk Privileged Identity Management (PSM) interface. In the background, a Notepad window shows a log of activities with columns for Time, User, and Action. The activities listed include 'PSM Connect', 'Use Password', and 'PSM Disconnect'. Overlaid on this is the 'Secure Connect' dialog box, which contains the following fields:

- Client: RDP
- Address: 19.168.41.63
- User Name: administrator
- Password: [masked]
- Logon To: abc_dom
- Port: 3389
- Map local drives:
- Connect to machine console:

Buttons for 'Connect' and 'Clear' are visible at the bottom of the dialog. A copyright notice at the bottom reads: 'Copyright © 1999-2012 CyberArk® Software, Ltd. All Rights Reserved.'



PSM – расследование инцидентов

Monitor

The screenshot displays the CyberArk Privileged Identity Management (PSM) interface. A central window titled "042a667d-ec43-4d8c-aa44-218e308627cb.VID.avi" shows a terminal session recording. The terminal output includes a table of employee data with columns "FIRST_NAME" and "SALARY". The table lists 20 employees with their respective salaries. Below the table, the terminal shows the command "SQL>" and a status message "107 rows selected." The recording player interface includes a progress bar and a time indicator "00:34 / 00:38". To the right of the recording player is a "Timeline" view showing a list of recording segments with their durations and offsets. The segment at 00:00:34 is circled in red. The interface also features a search panel on the left with filters for "Sessions" (oracle) and "Commands and Events" (salary). The top of the window shows the date "11/3/2011" and navigation links for "About", "Logout", "auditor", and "Help".

FIRST_NAME	SALARY
Sundar	43120
Anit	43120
Lisa	85000
Harrison	85000
Taylor	43120
William	43120
Elizabeth	85000
Sudha	43120
Elle	85000
Alyssa	17999
Jessathon	16000
Fach	13466
Madhurely	25000
Charles	25000
Winston	43120
Jean	25000
Martha	52300
Girard	12246
Mandita	52522
Alain	14567
Sally	52300
Anthony	52300
Betty	17098
Jennifer	55567
Timothy	17098
Randall	23400
Sarah	17098
Britney	17098
Samuel	29120
Janece	29120
Alicia	23459
Kevin	29120
Donald	29120
Douglas	29120
Jennifer	23000
Michael	12010
Pat	29120
Steven	23000
Bernard	23000
Shelley	23000
William	23000

* Supports SSH and SQL commands

PSM – доступ к веб-сайтам и приложениям

Monitor

- Управляет учетными данными к веб-сайтам, веб-приложениям и SaaS
- Прозрачно подключает веб-приложениям без рас
- Заплай



	User Name	Address	Safe	Policy ID				
<input type="checkbox"/>	marketing@gmail.com	www.facebook.com	Passwords	Facebook				
<input type="checkbox"/>	KateM@acme.com	login.salesforce.com	Passwords	SalesForce				
<input type="checkbox"/>	KateM@acme.com	mysupport.mcafee.com	Passwords	McAfee				

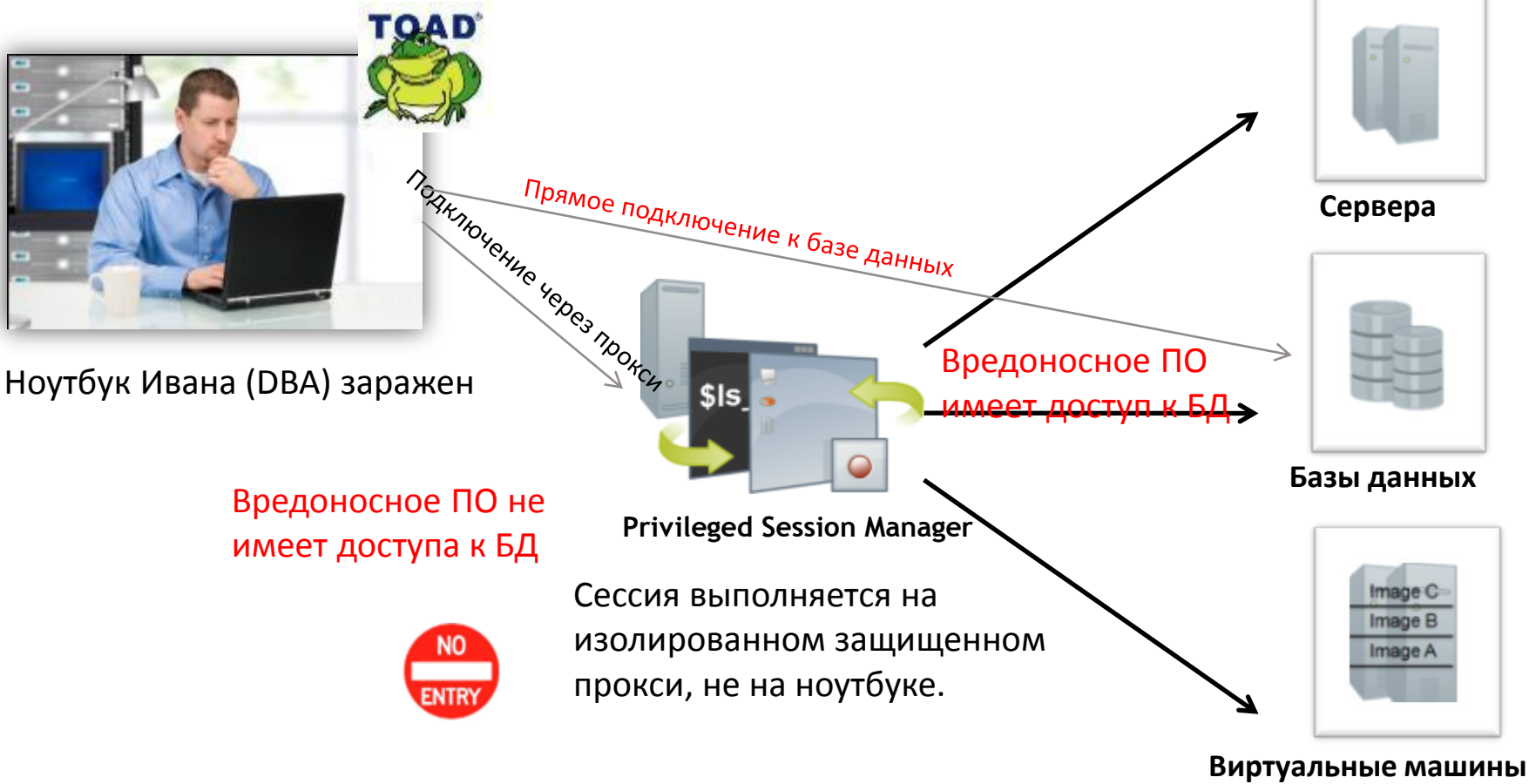


CYBERARK

PSM – изоляция нарушителя, предотвращение атак



Как снизить риск заражения систем?





CYBERARK

Sensitive Information Management (SIM)

MFT от CyberArk

Тысячи передаваемых файлов ежедневно...



Поставщики



Консультанты



Провайдеры



Партнеры



Правительство



Банки



Типографии



Юристы



Страхование



Процессинг

Решения для безопасного обмена файлами ?

Ручные процессы и высокая стоимость поддержки



FTP/Secure FTP

Не отслеживается

Не безопасен

Без централ. управления

Стоимость курьерских служб и выделенных линий



Бесплатные веб-серверы

Потеря контроля и доверия

Не интегрируются с корпоративными системами

Задержки бизнеса по причинам IT

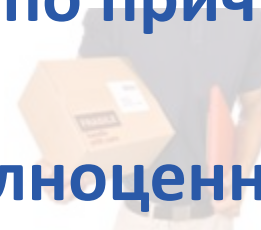


Домороженное ПО

Дорогая поддержка

Сложно для compliance

Нет мониторинга и полноценного аудита



Курьерские службы

Дорого

Задержка доставки

Проблемы получения

Финансовые потери и хищения



Email

Не безопасна

Ограничения объема

Высокие штрафы за несоответствие



Fax

Ручные процессы

Нет резервных копий

Репутационные риски



Выделенные линии

Дорого



В идеале MFT-решение...

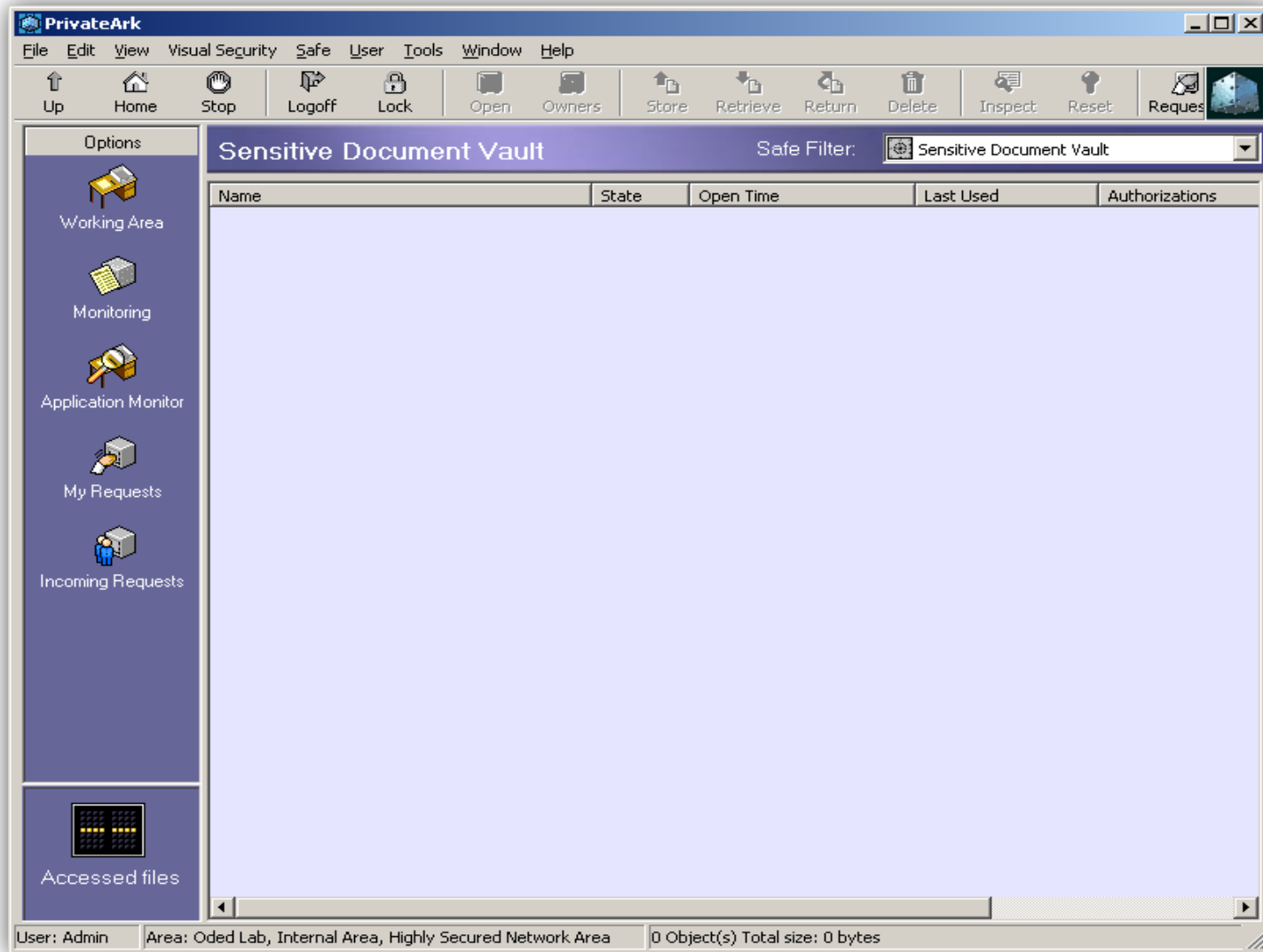
1. Отчетность по состоянию системы и операциям с файлами
2. Неотказуемость отправителя и получателя
3. Возможность проведения аудита
4. Глобальную доступность
5. Автоматизацию передач файлов и отправки уведомлений
6. Защищенность интерфейсов отправителя и получателя
7. Метрики и мониторинг производительности
8. Поддержку различных протоколов передачи файлов
9. Безопасную передачу файлов через не доверенные сети
10. Безопасное хранение файлов
11. Аутентификацию пользователей в LDAP/Active Directory
12. Интеграцию с использованием документированного API
13. Гибкое конфигурирование



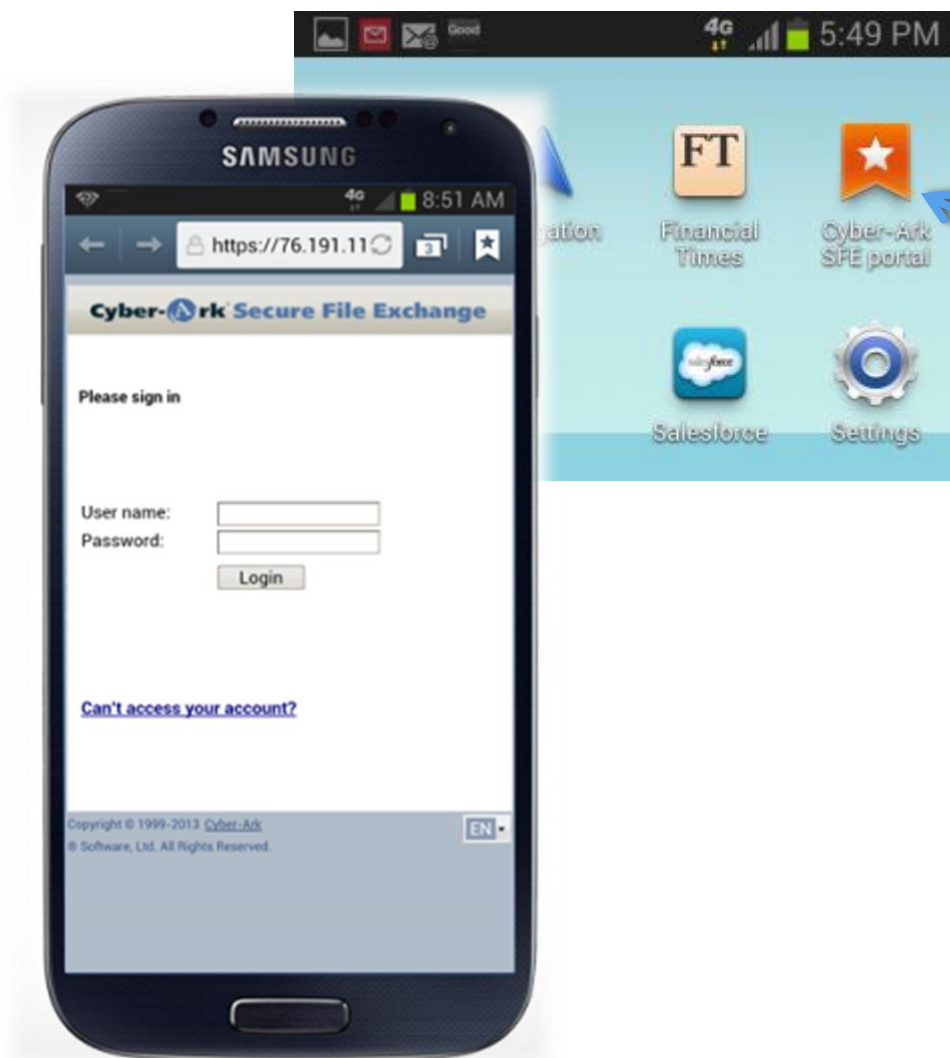
SIM - MFT от CyberArk



Защищенность: администратору нет доступа к данным

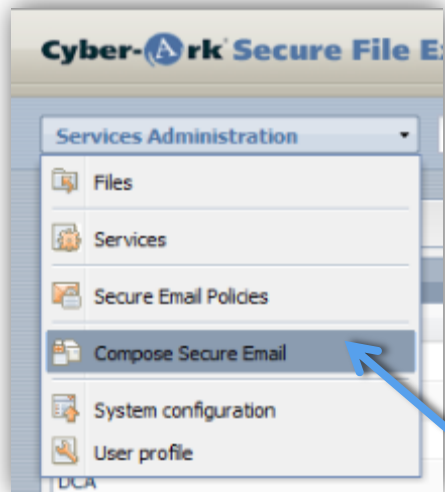


Работа с любых платформ



**Легкий способ
создать ярлык в
любом
мобильном
устройстве**

Создание Secure Email в любом месте и время



Secure Compose

Add Cc Add Bcc

From: On behalf of y@y.com

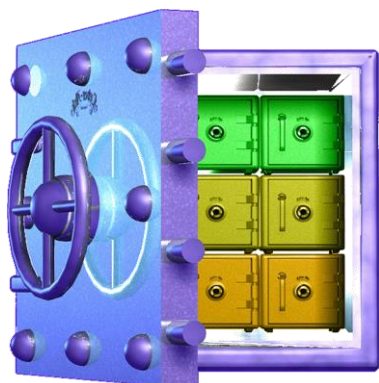
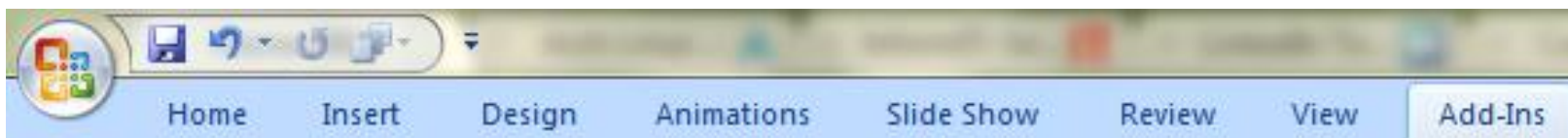
To:

Subject:

Send me a copy of this reply

Непосредственно из SFE.
Удобно для Mac и Lotus notes

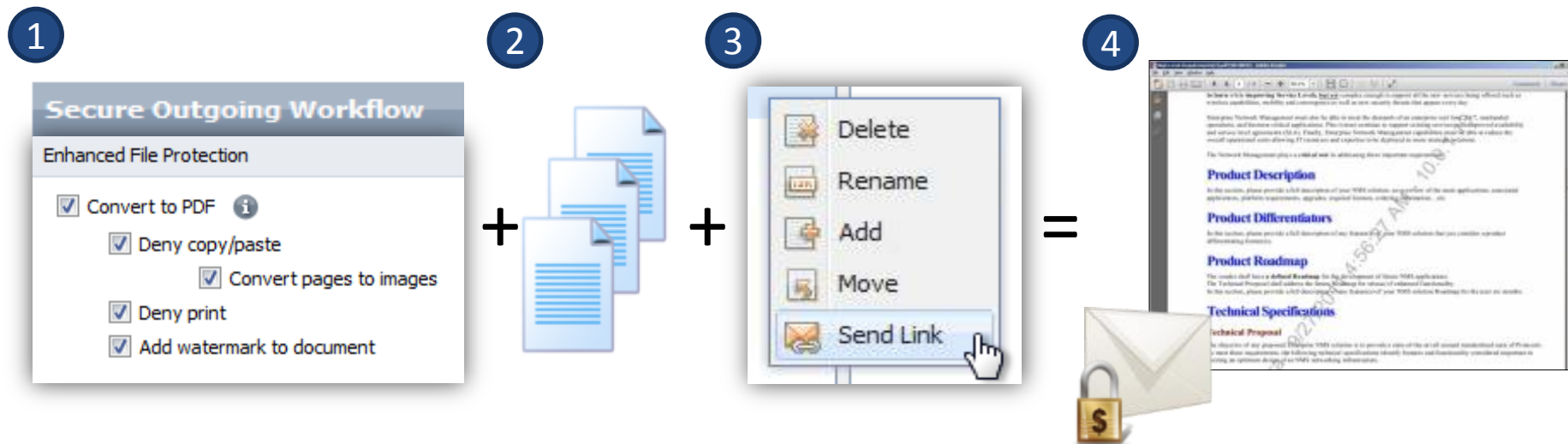
SIM – готовая интеграция



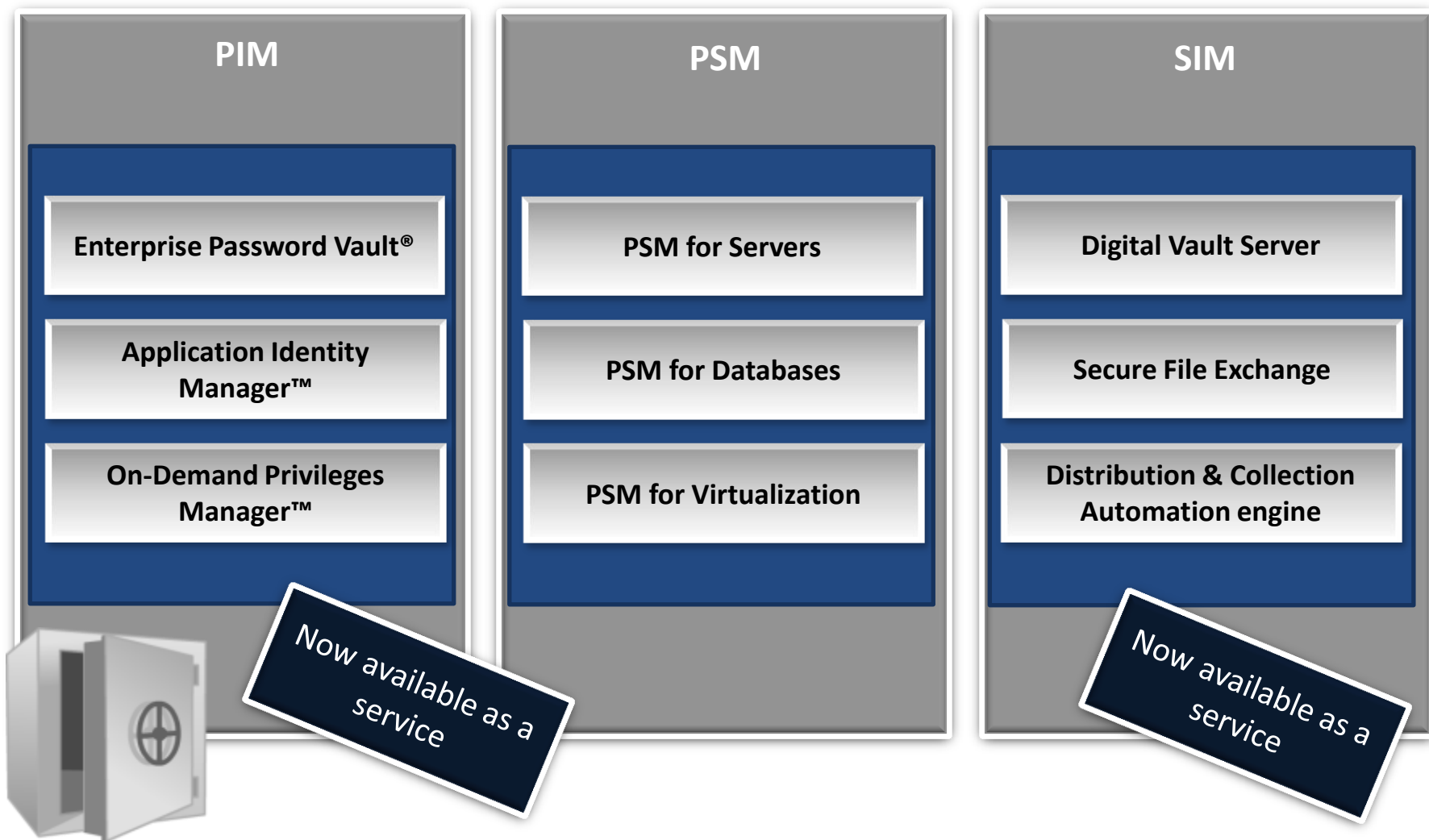
Элементарно, для бизнес-пользователей

- Павел, CFO отправляет конфиденциальный отчет для изучения советом директоров

Отправлена ссылка на отчет с ограничением на просмотр

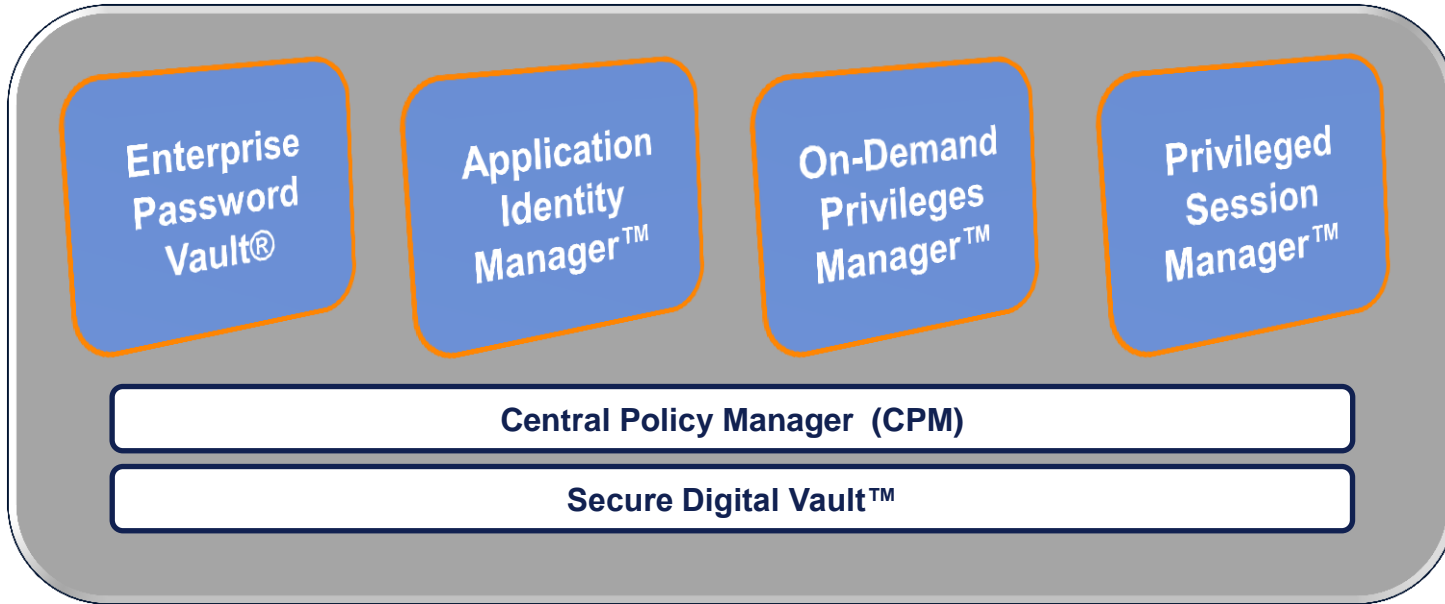


Решения CyberArk



Лицензирование PIM for Hosting Providers

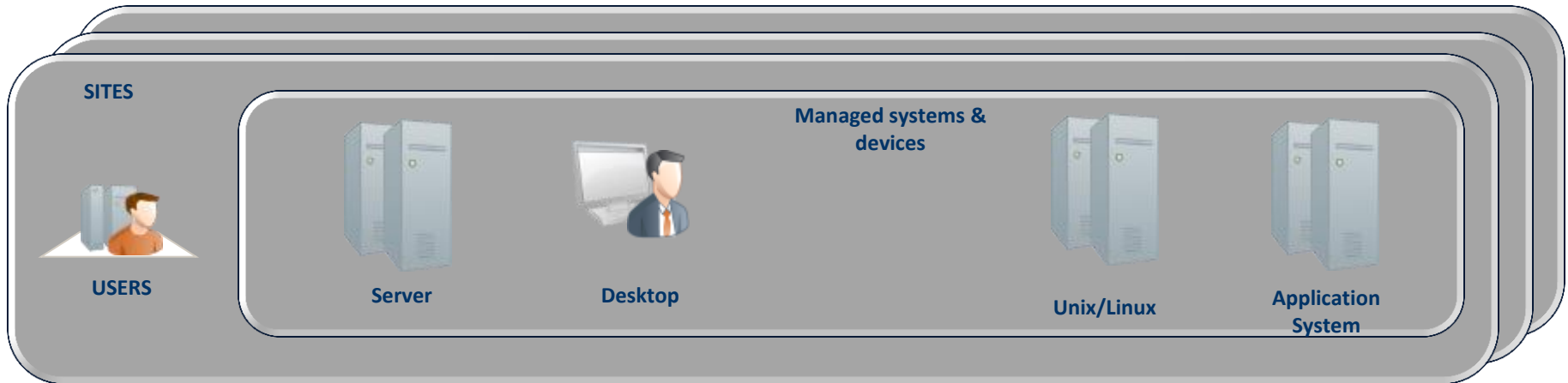
Annual subscription for hosting service providers



CPM



Digital Vault



Лицензирование SIM-as-a-Service

Hosted instance of SIM on an annual subscription basis



CYBERARK®



CYBERARK

Спасибо за внимание...