Création, Sécurisation, Traçabilité des mots de passe : Une situation totalement sous contrôle ?

Bruno RASLE
bruno.rasle@cortina.fr

A votre disposition :

- Etude Cyber-Ark « *Password Survey 2007* »
- Livre blanc « *Audit de mots de passe* »
- Livre blanc « *Vive les mots de passe* »

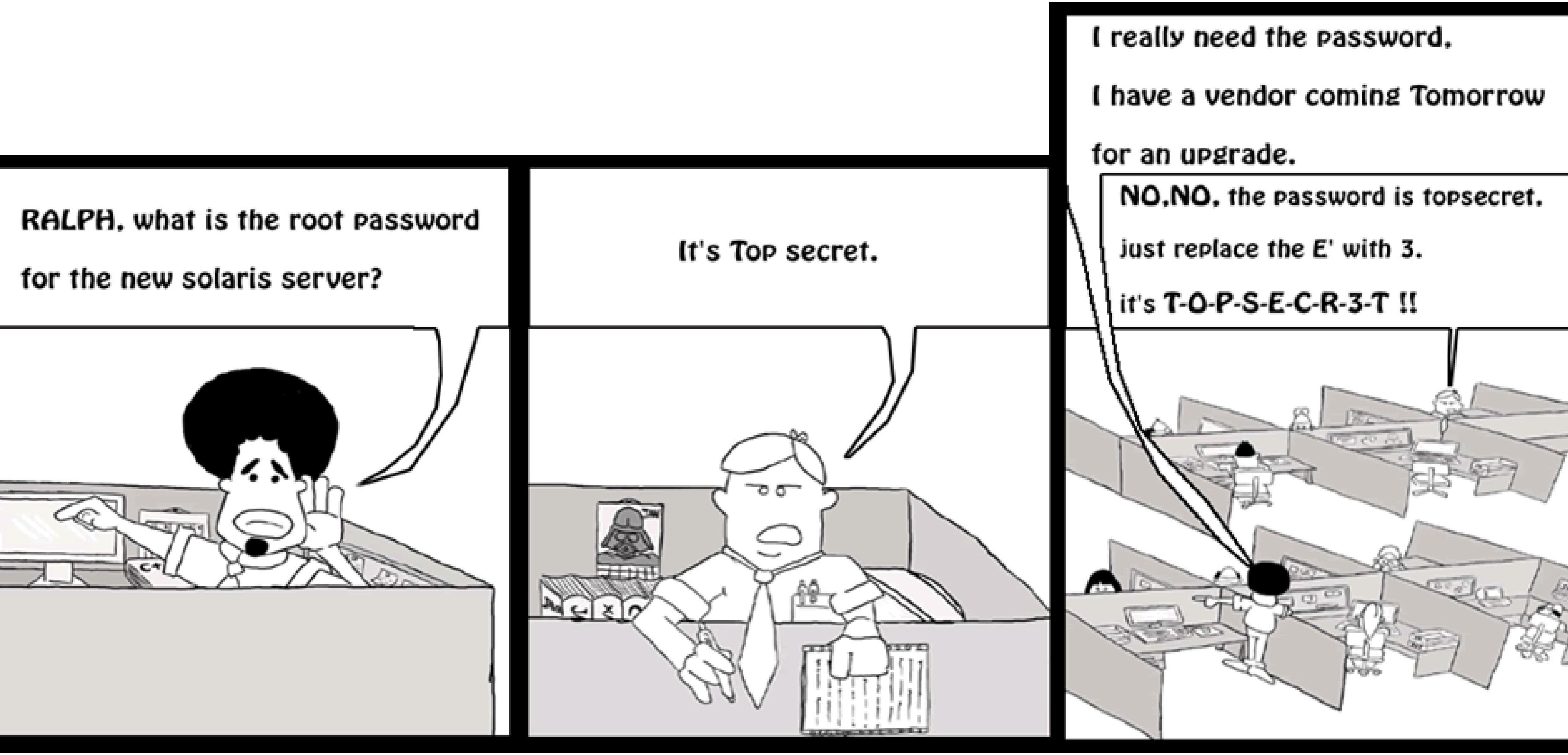
www.cortina.fr

OSSIR – 11 juin 2007

Managing Privileged Accounts

Calum MacLeod
VP Europe and Africa
calum.macleod@cyber-ark.com
+31621827253

www.cortina.fr


RALPH, what is the root password for the new solaris server?
It's Top secret.
I really need the password. I have a vendor coming Tomorrow for an upgrade.
NO,NO, the password is topsecret. just replace the E' with 3. it's T-O-P-S-E-C-R-3-T !!

Agenda

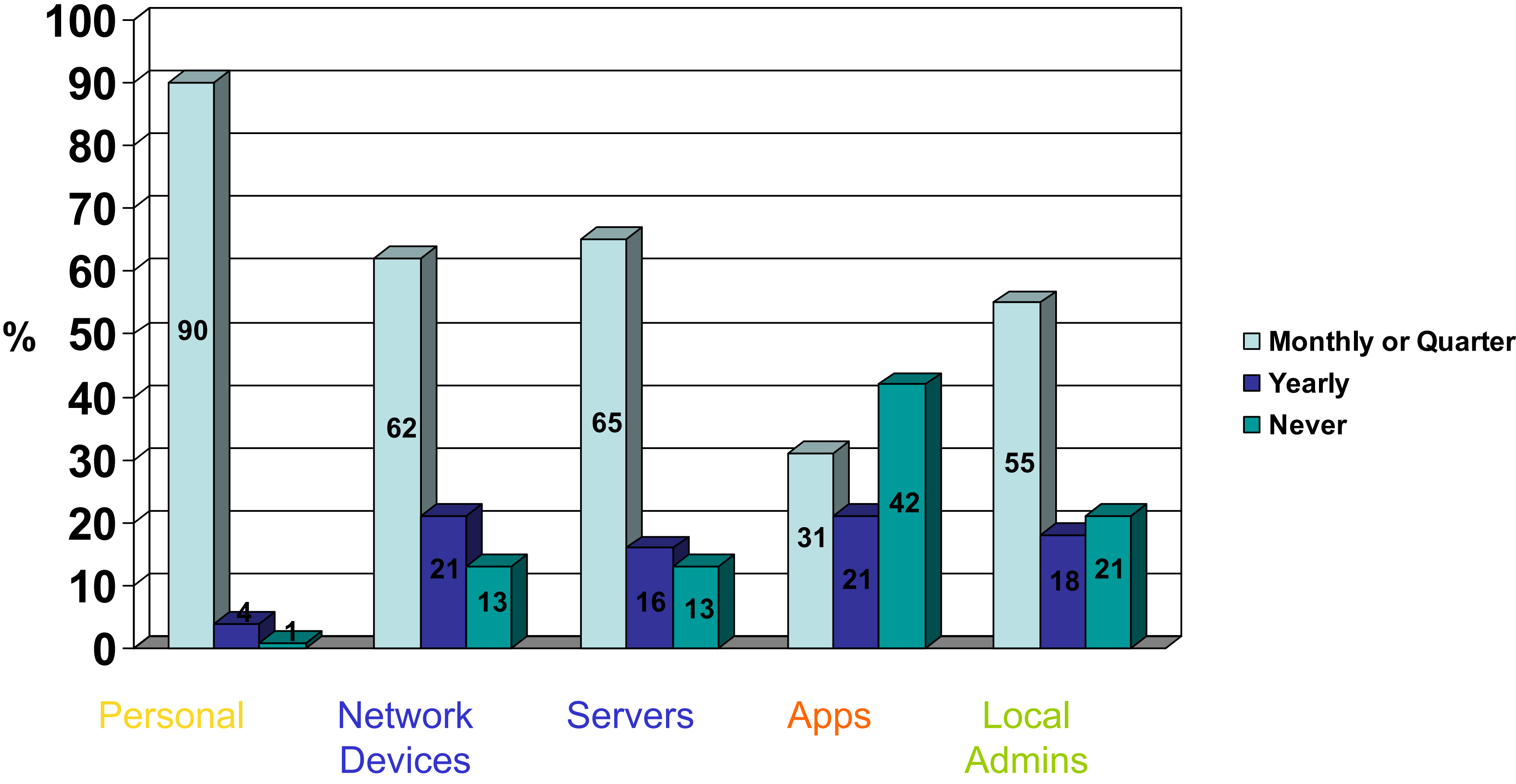
1. What problems stem from the spread of superuser privileges and shared privileged accounts?
2. How can you better manage service account passwords?
3. What solutions can you use to better manage these privileges and accounts?

Source - Gartner

What problems stem from the spread of superuser privileges and shared privileged accounts?

Policies For Regular Accounts Are Not Implemented For Privileged Accounts

Password reset frequency



Privileged Account Types

Administrative Accounts

Shared Predefined:

- UNIX root
- Cisco enable
- DBA accounts
- Windows domain
- Etc.

Shared:

- Help Desk
- Fire-call
- Operations
- Emergency
- Legacy applications
- Developer accounts

Owned by the system:

- Not owned by any person or “identity”

Application Accounts

Hard-coded, embedded:

- Resource (DB) IDs
- Generic IDs
- Batch jobs
- Testing Scripts
- Application IDs

Service Accounts:

- Windows Service Accounts
- Scheduled Tasks

Personal Computer Accounts

Windows Local administrator:

- Desktops
- Laptops

One Rule for the Privileged… '

- Users with superuser (administrator, root) and similar privileges can do a lot of damage…
- But many organizations subject ordinary users to greater rigour!
- Why do so many users have superuser privileges when they don't need (all of) them (all of the time)?
- Why are so many superuser accounts – and hence, passwords – shared?

Source - Gartner

Cause and Effect

- Study from December 19th 2006 - Source CERT
  - Insiders were disgruntled and motivated by revenge for a negative work-related event.
  - Insiders exhibited concerning behavior prior to the attack.
  - Insiders who committed IT sabotage held technical positions.
  - The majority of the insiders attacked following termination

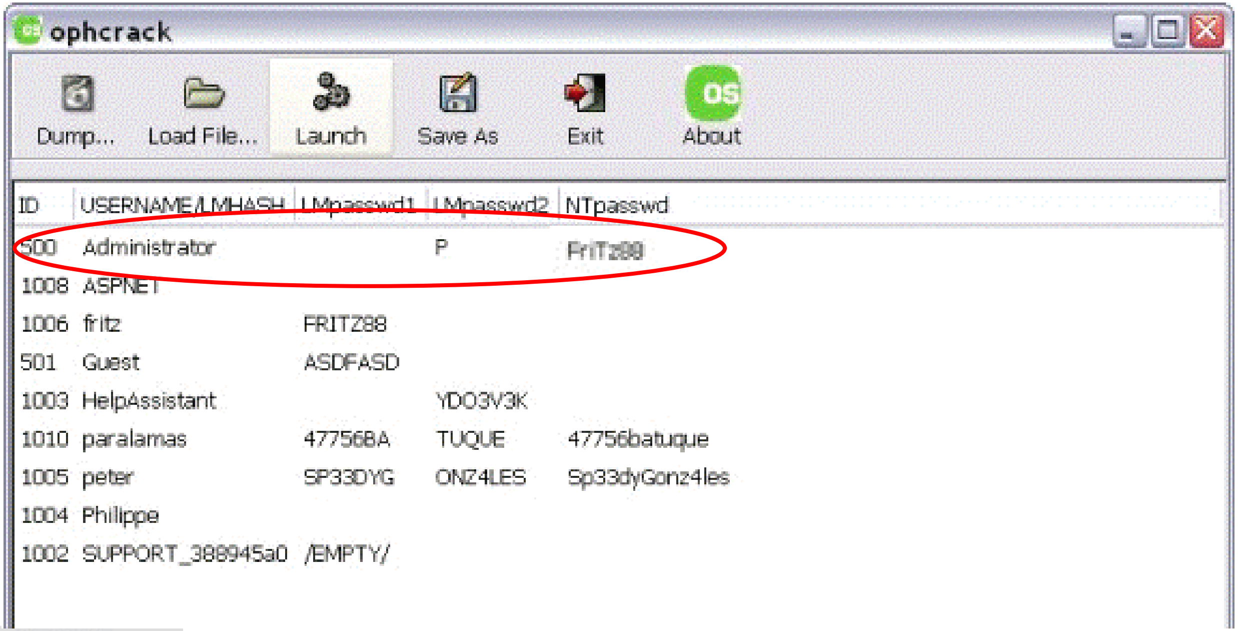
Where’s Your REAL Risk

- 86% of the insiders held technical positions,
- 90% were granted system administrator or privileged system access.
- 59% of the insiders were former employees,
- 57% should not have authorized system access at the time of the attack,
- 64% used remote access.

How to Easily Access any Windows Machine in the Network - I

Step 1 –

Many cracking tools for Windows local users are available on the web. Any insider can use them to crack the local Administrator password on **her** own laptop/desktop…



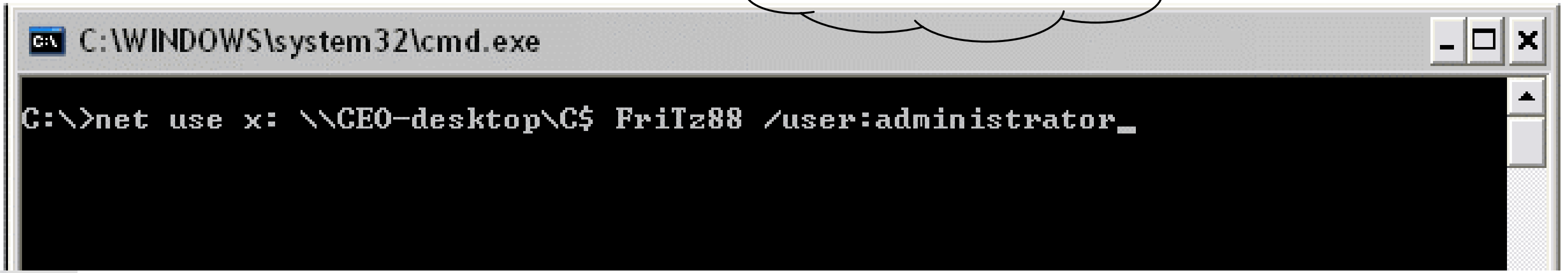
ID	USERNAME/LMHASH	LMpasswd1	LMpasswd2	NTpasswd
500	Administrator		P	FriTz88
1008	ASPNET			
1006	fritz	FRITZ88		
501	Guest	ASDFASD		
1003	HelpAssistant		YDO3V3K	
1010	paralamas	47756BA	TUQUE	47756batuque
1005	peter	SP33DYG	ONZ4LES	Sp33dyGonz4les
1004	Philippe			
1002	SUPPORT_388945a0	/EMPTY/		

How to Easily Access any Windows Machine in the Network - II

Step 2 –

Since it is the same password being used across the organization for all local administrators, the user can now remotely access any desktop with administrator permissions!

CEO desktop



```
C:\>net use x: \\CEO-desktop\C$ FriTz88 /user:administrator_
```

Problems With Reckless Superuser Privileges

- MOST SERIOUS violation of the principle of least privilege
- Huge opportunity for security breaches through ignorance, accident or malice
- High privacy risk through access to sensitive personal data (medical, financial, R&D, etc.)
- High compliance risk through access to financial systems, cardholder data, etc.

➔ *Can you provide individual users with just the superuser privileges they need?*

Source - Gartner

➔ *And only when they need them?*

Multi-facet problem requires comprehensive solution

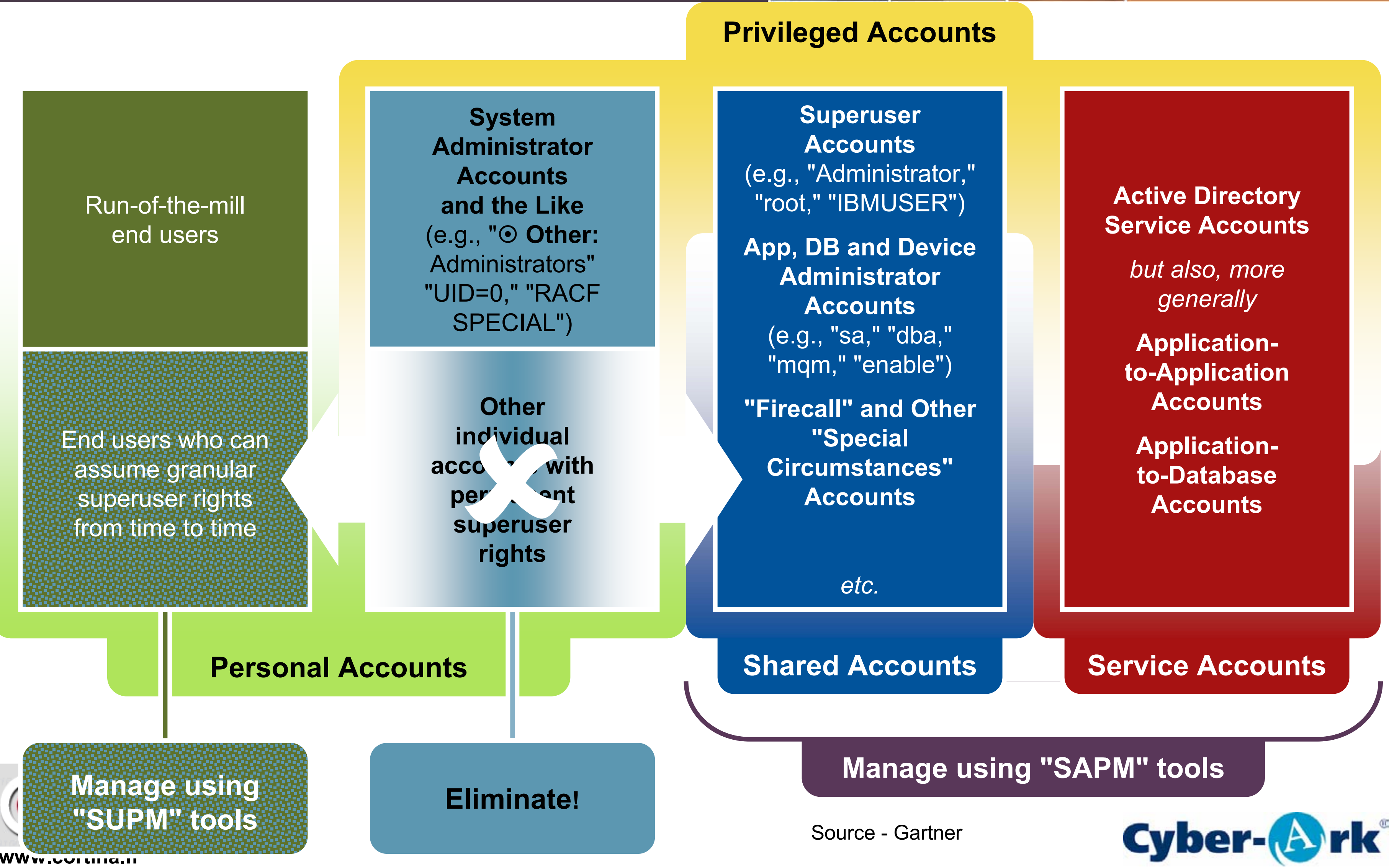
	Which	Problems	Requirements
Administrative	• Servers • Network appliances • Databases	• Highly powerful • Shared • Recurring • Easy to guess • Rarely changed	• Personal accountability • Highly secure long-term storage • Dual control release mechanism • Accessibility on disaster recovery scenarios • Frequent resets
Applications	• Application IDs • Scripts • Batch jobs • Service accounts • Scheduled tasks	• Stored in clear text • Risky to change • Difficult to change • Shared	• Automatic mechanism to facilitate periodic resets • To be hidden from developers and support stuff
Personal Computers	• Local admins	• Highly powerful • Widely known • Recurring • Easy to guess • Rarely changed	• Temporary access for helpdesk and field technical staff (fire-call) • Personal accountability • Automatic and managed reset process • Dual control release mechanism

How Can You Better Manage Service Account Passwords?

Managing The Problem

1. Count your privileged passwords
2. Personalize who has privileged or super user access
3. Disable inactive accounts
4. Make sure that passwords are changed on a regular basis
5. Don’t forget embedded accounts
6. Automate, automate, automate

The User Community



Privileged Accounts

Run-of-the-mill end users

End users who can assume granular superuser rights from time to time

System Administrator Accounts and the Like (e.g., "⦿ **Other:** Administrators" "UID=0," "RACF SPECIAL")

~~**Other individual accounts with permanent superuser rights**~~

Superuser Accounts (e.g., "Administrator," "root," "IBMUSER")

App, DB and Device Administrator Accounts (e.g., "sa," "dba," "mqm," "enable")

"Firecall" and Other "Special Circumstances" Accounts

etc.

Active Directory Service Accounts

but also, more generally

Application-to-Application Accounts

Application-to-Database Accounts

Personal Accounts

Shared Accounts

Service Accounts

Manage using "SUPM" tools

Eliminate!

Manage using "SAPM" tools

Source - Gartner

Cyber-Ark

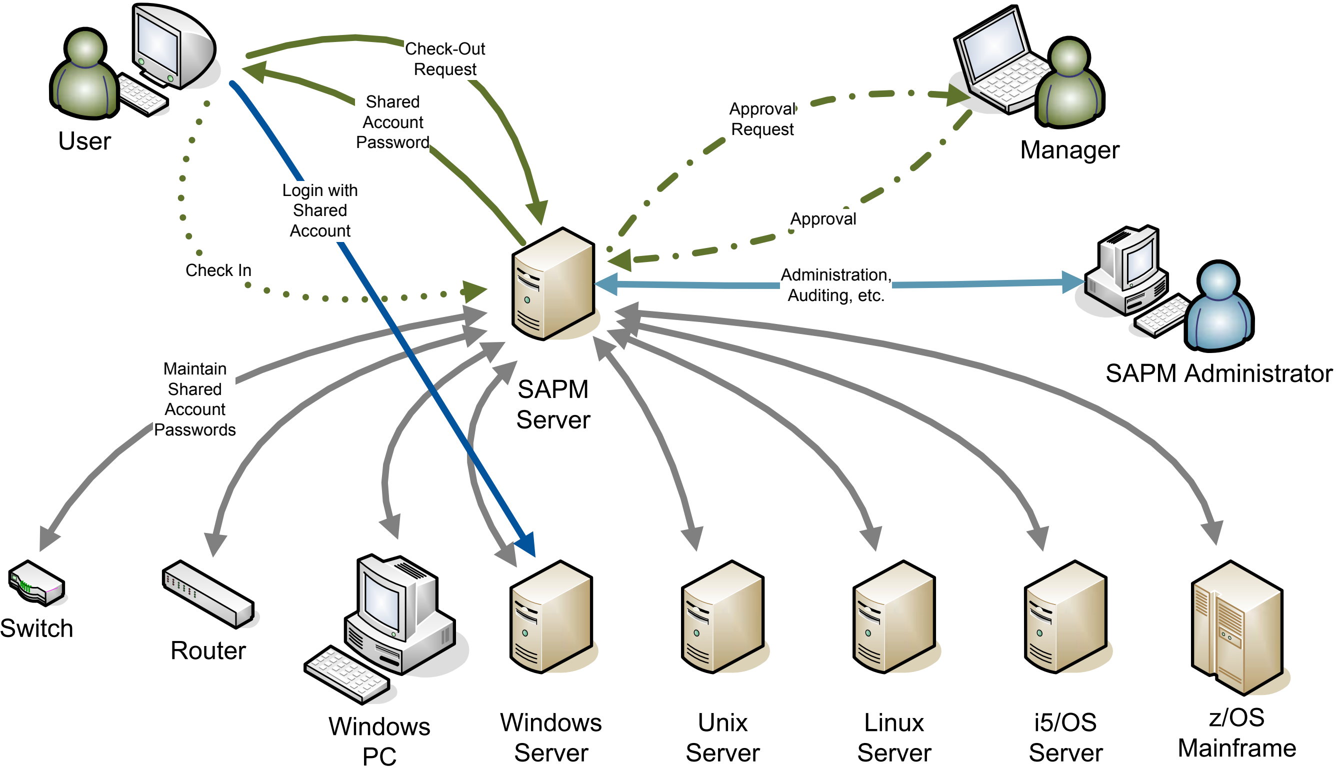
www.cortina.it

What Solutions Can You Use To Better Manage These Privileges And Accounts?

What Is Required?

- Enterprise policy enforcement
  - Frequent Auto Change
  - Dual Control
  - One-time Password
  - Unique strong password
- Strong auditing
  - Personalization
  - Secured sharing
- Business continuity
  - Long-term Storage
  - Availability during Disaster Recovery

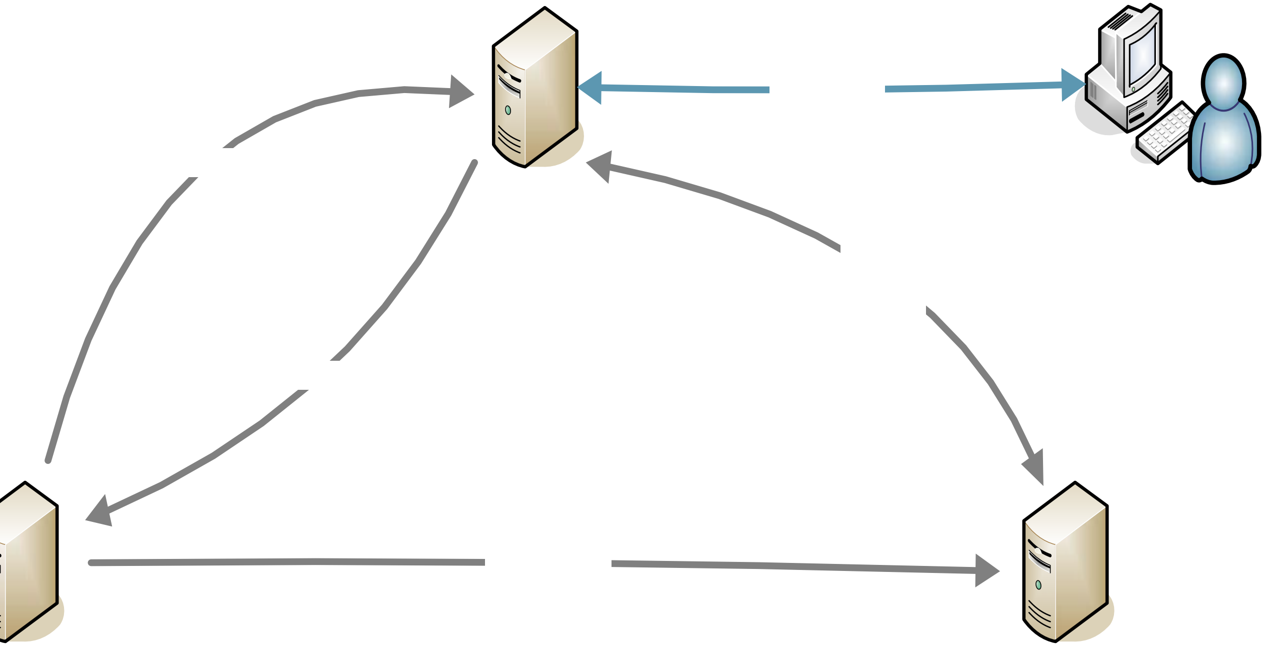
SAPM/PPM Tools



Source - Gartner

- Users can "check out" specified shared accounts
- Check-out request may need manager's (or other's) approval (dual control)
- Shared-account password released to the user, who can log in with that account
- Request is logged ➔ user is accountable
- SAPM server resets password when user "checks in" or after a preset time

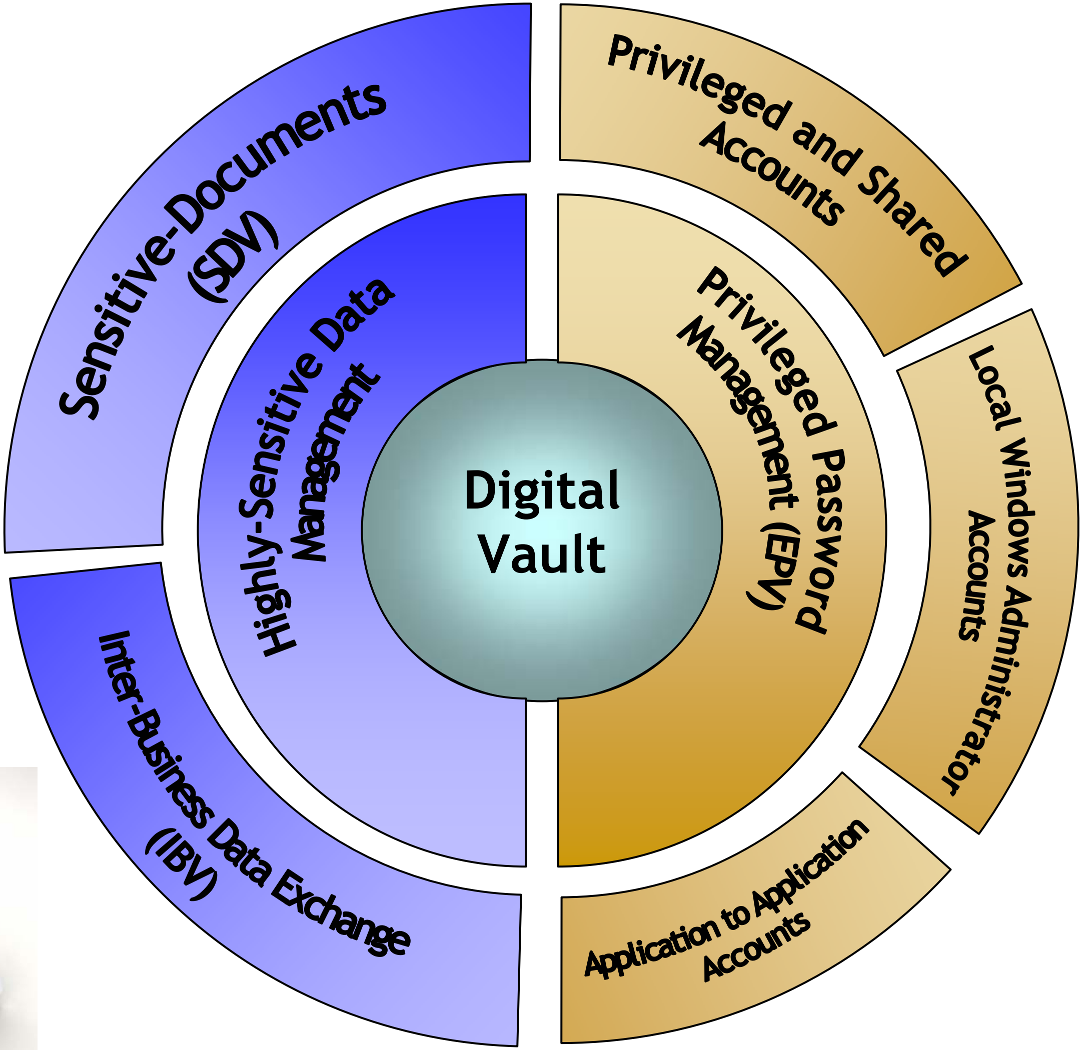
Service Account Password Management



- Requesting application retrieves service account password from SAPM server
- Application needn't even know the service account username – can request using alias
- Application logs in with username and password retrieved from SAPM server

Source - Gartner

Cyber-Ark Products



Digital Vault

Highly-Sensitive Data Management

Privileged Password Management (EPV)

Sensitive-Documents (SDV)

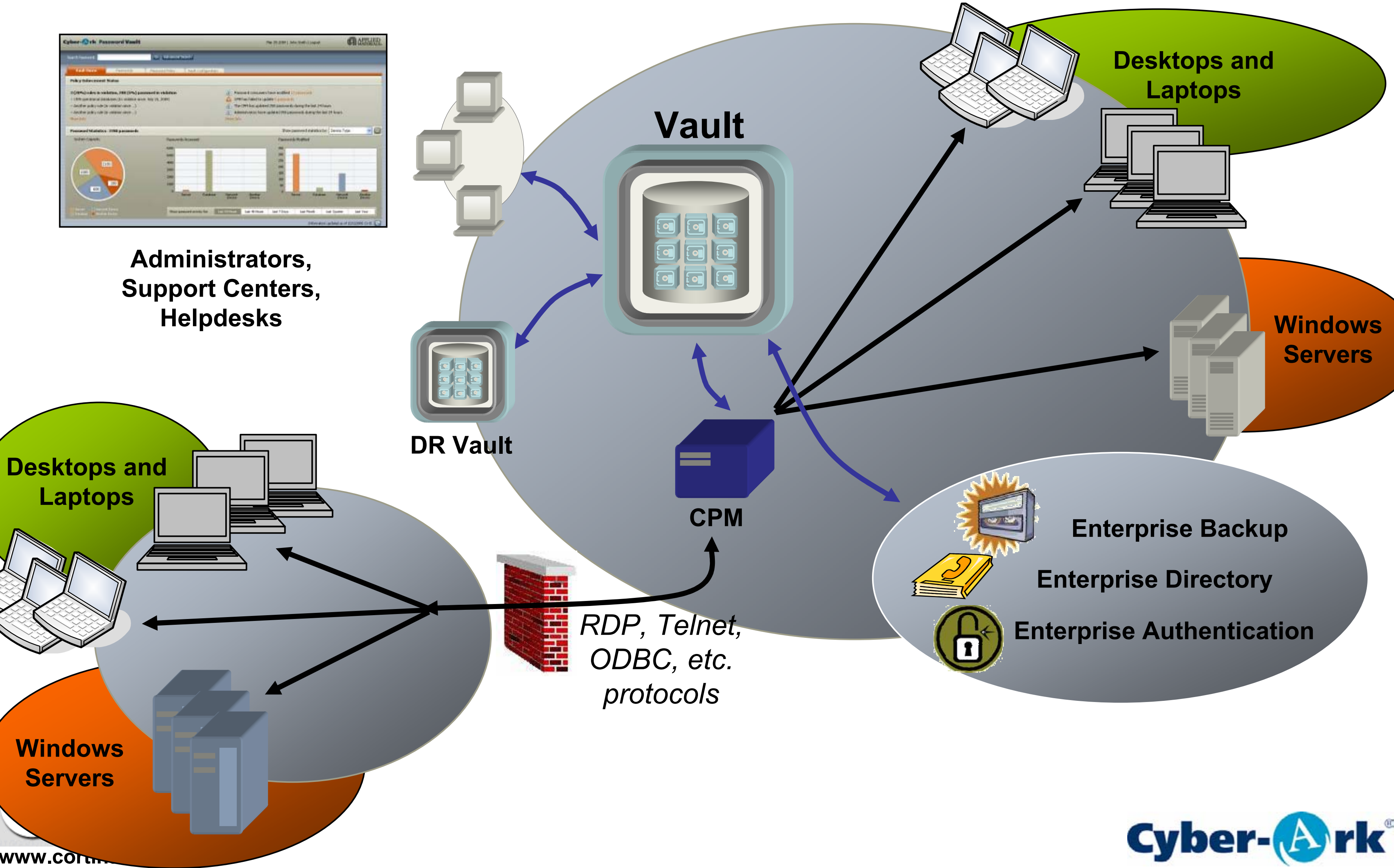
Privileged and Shared Accounts

Local Windows Administrator Accounts

Application to Application Accounts

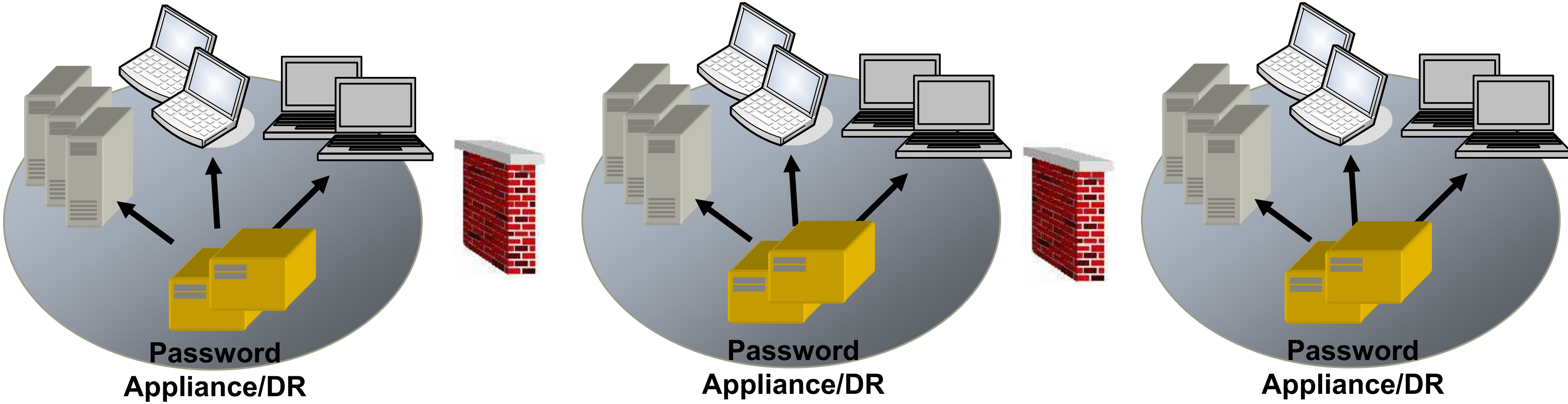
Inter-Business Data Exchange (IBV)

Windows Local Administrators
Simple Architecture

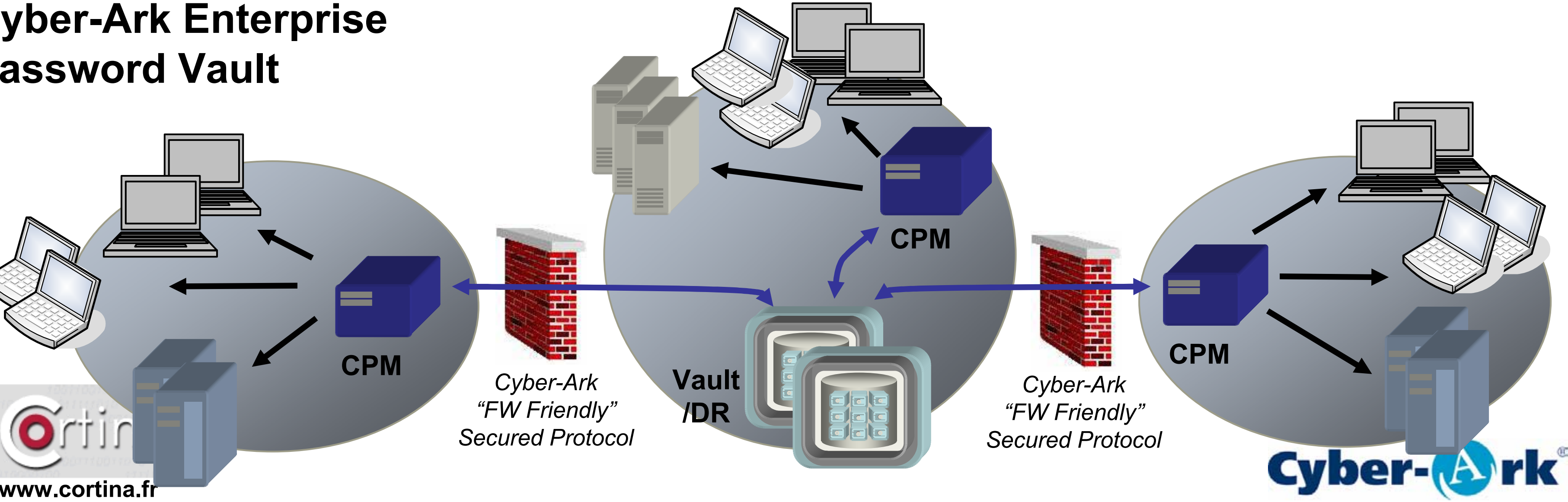


Distributed Architecture

ll-in-one Solutions

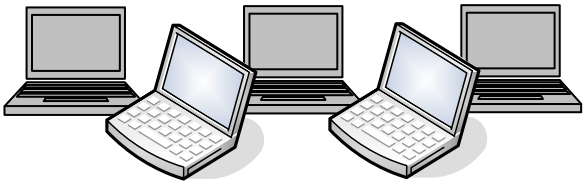


yber-Ark Enterprise assword Vault

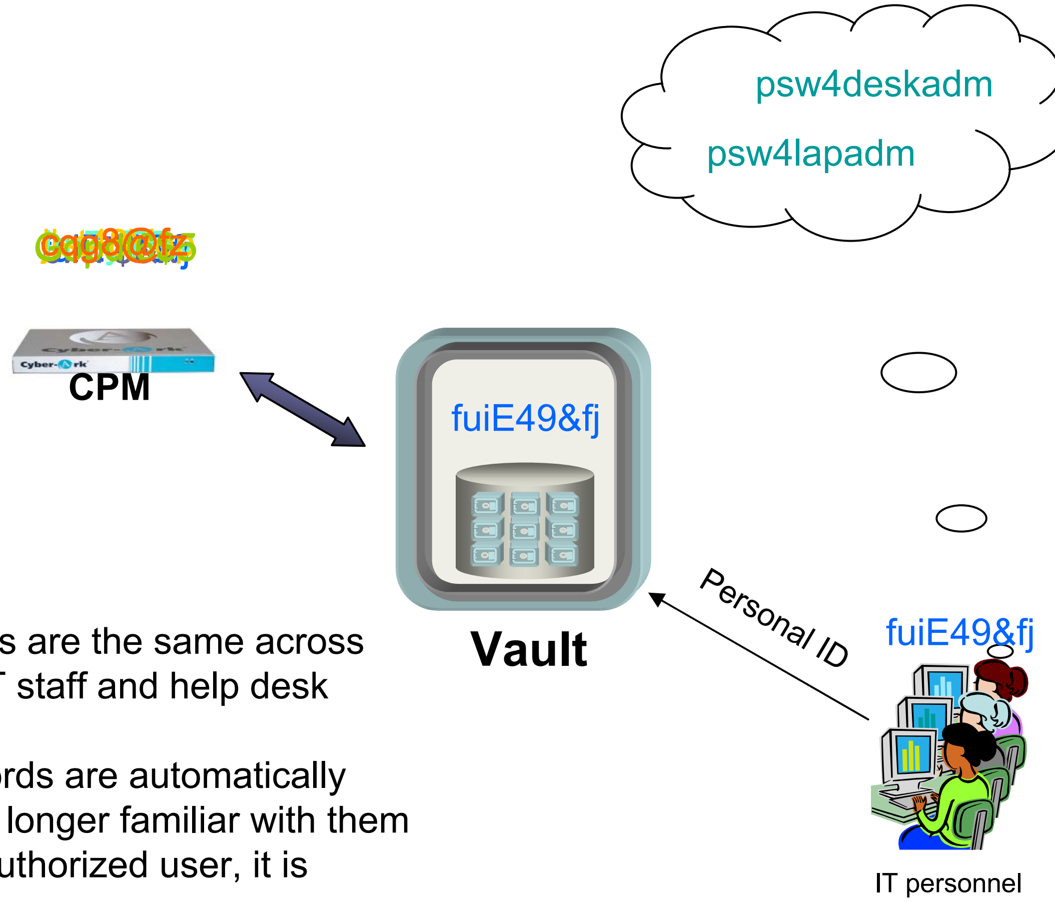

CPM
CPM
CPM
Cyber-Ark "FW Friendly" Secured Protocol
Vault /DR
Cyber-Ark "FW Friendly" Secured Protocol

Windows Local Administrators
Concept of Operation

System	User	Pass
Desktop A	Administrator	psw4deskadm
Desktop B	Administrator	psw4deskadm
Desktop C	Administrator	psw4deskadm
Laptop D	Administrator	psw4lapadm
Laptop E	Administrator	psw4lapadm

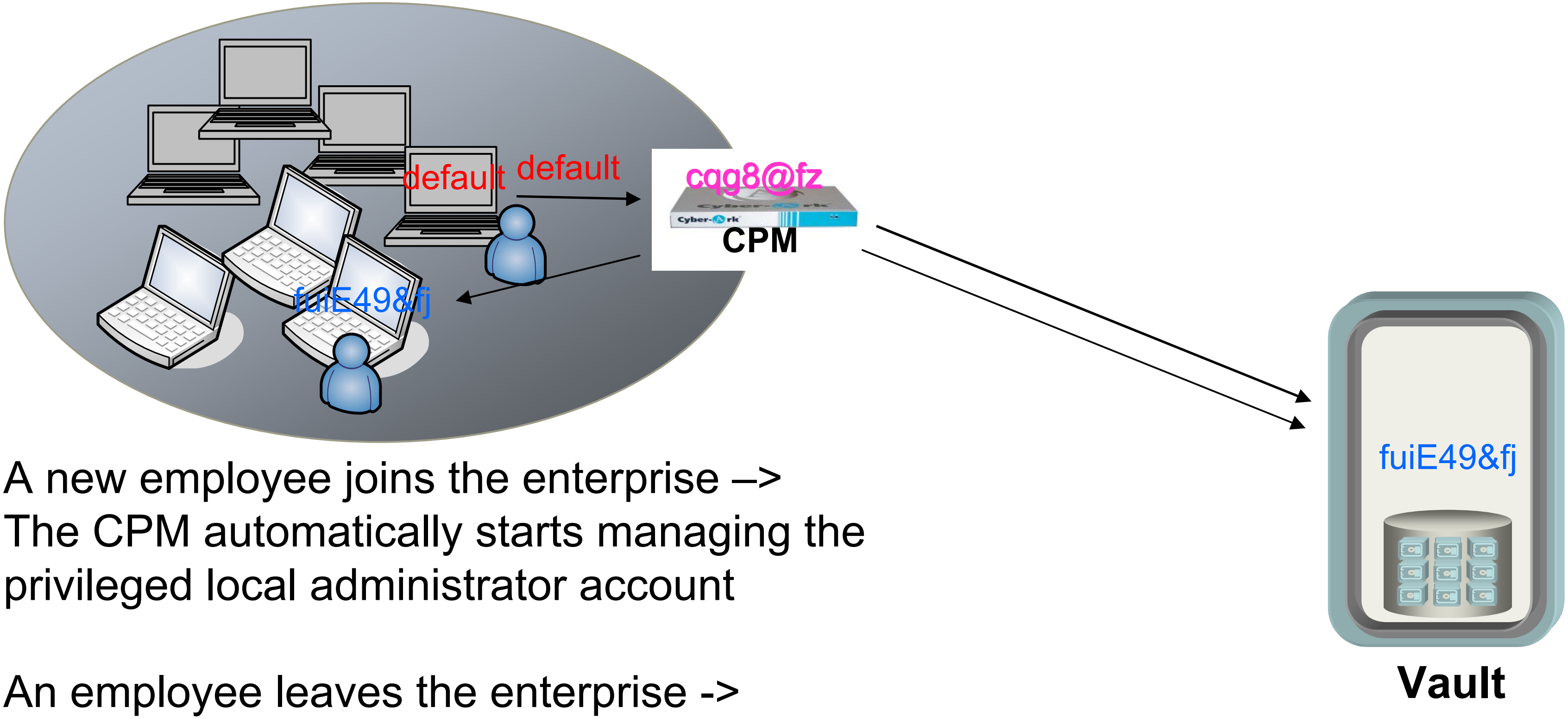


Desktops & Laptops



- Until today – local administrator passwords are the same across enterprise desktops/laptops and usually IT staff and help desk personnel memorize them
- Using the EPV solution – different passwords are automatically generated for each PC and IT staff are no longer familiar with them
- Whenever a password is required by an authorized user, it is checked-out from the Vault
- It is then used on the desktop or laptop and automatically changed upon check-in

Windows Local Administrators
Automatic Machines Detection



- A new employee joins the enterprise –> The CPM automatically starts managing the privileged local administrator account
- An employee leaves the enterprise -> The CPM automatically archives the relevant machine (password) in the Vault

Contrôle hiérarchique

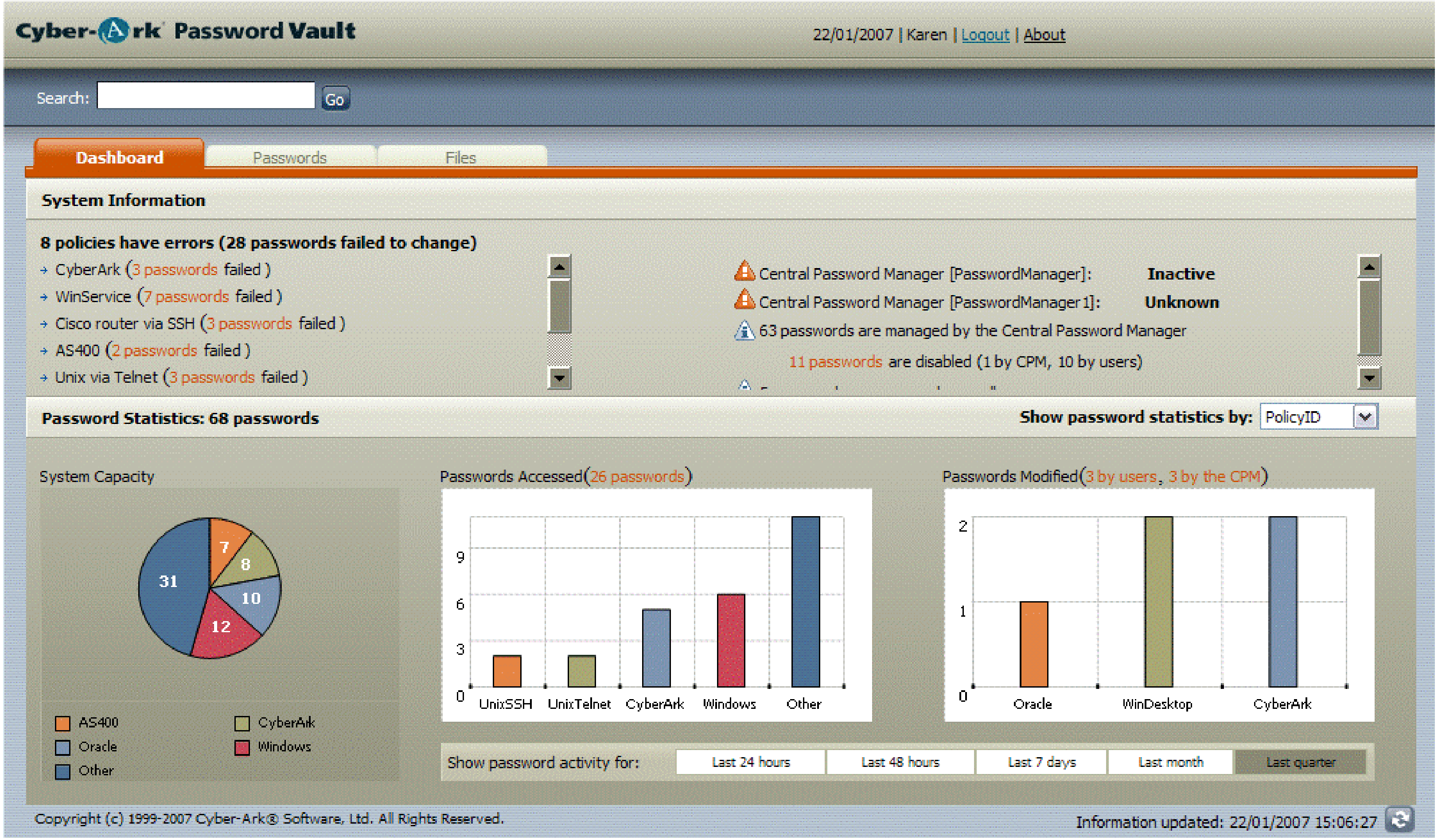
Responsable Oracle

DBA Oracle

DRH, ou DAF

“Data Owner”

Tableau de bord



Cyber-Ark Password Vault

22/01/2007 | Karen | Logout | About

Search: [ ] Go

Dashboard | Passwords | Files

System Information

8 policies have errors (28 passwords failed to change)

- CyberArk (3 passwords failed)
- WinService (7 passwords failed)
- Cisco router via SSH (3 passwords failed)
- AS400 (2 passwords failed)
- Unix via Telnet (3 passwords failed)

⚠ Central Password Manager [PasswordManager]: **Inactive**

⚠ Central Password Manager [PasswordManager1]: **Unknown**

⚠ 63 passwords are managed by the Central Password Manager

11 passwords are disabled (1 by CPM, 10 by users)

Password Statistics: 68 passwords

Show password statistics by: PolicyID

System Capacity

🟧 AS400
🟨 CyberArk
🟦 Oracle
🟥 Windows
🟦 Other

Passwords Accessed(26 passwords)

Passwords Modified(3 by users, 3 by the CPM)

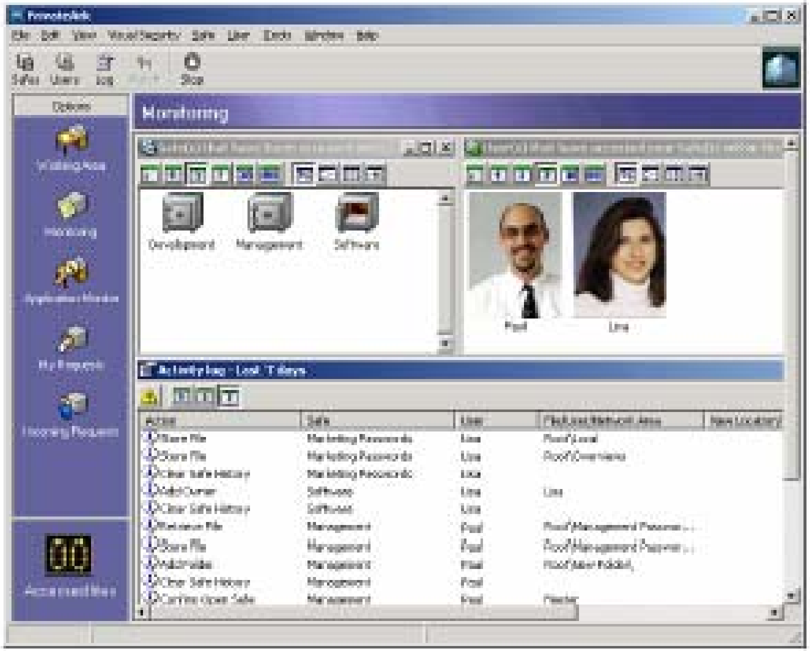
Show password activity for: Last 24 hours | Last 48 hours | Last 7 days | Last month | Last quarter

Information updated: 22/01/2007 15:06:27

Audit et Reporting

«Nos bases de données sont stratégiques. Je veux savoir lesquelles ont été accédées, par quel administrateur, quand, pour quelle raison et d'où la demande été faite »

- Retour de congés
- Activité par cible
- Activité par Administrateur
- Utilisateurs activés
- Par raison
- Créations et modification, etc.



Activity log - Last 7 days

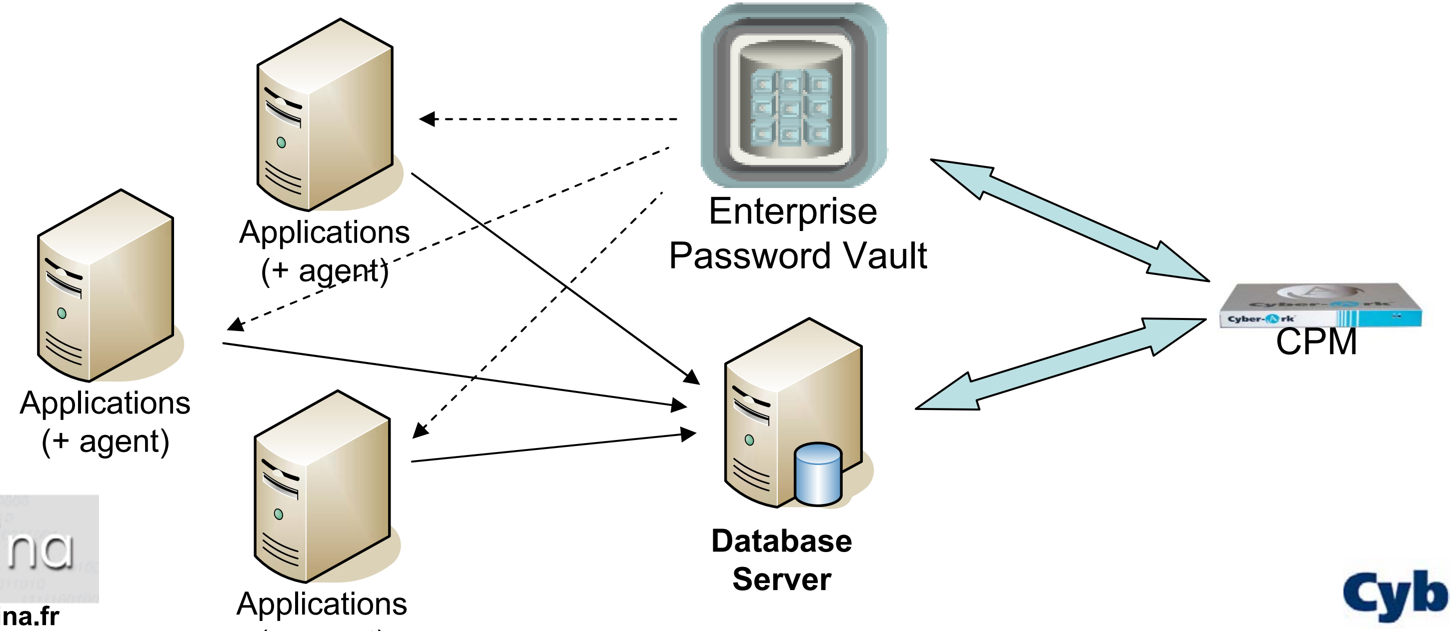
Action	Safe	User	File/Location/Network Area	New Location
Store File	Marketing Passwords	Lisa	Root\Local	
Store File	Marketing Passwords	Lisa	Root\Overview	
Clear Safe History	Marketing Passwords	Lisa		
Add Owner	Software	Lisa	Lisa	
Clear Safe History	Software	Lisa		
Retrieve File	Management	Paul	Root\Management Passwor...	
Store File	Management	Paul	Root\Management Passwor...	
Add Folder	Management	Paul	Root\New Folder1,	
Clear Safe History	Management	Paul		
Confirm Open Safe	Management	Paul	Monitor	

Application Passwords

- Scripts & Jobs
  - Shell, Perl, Bat, Sqlplus, JCL…
- Applications
  - Custom developed C/C++, COM, Java, .NET code, Cobol
  - ERP systems
- Application Servers
  - WebSphere, WebLogic, Oracle Application Server…
- Products
  - IT Management tools
  - ETL tools (Informatica, IBM DataStage, etc…)

Architecture

- Agent
  - Manages and protects password cache
  - Provides high-availability
  - Authenticates calling applications
- Application
  - Requests credentials from the agent via API/CLI
- Vault/CPM
  - Store all credentials and manage password replacement processes



Hard-Coded Password Embedded in Code

```
.
.
UserName = “app”
Password = “asdf”
Host = “10.10.3.56”
ConnectDatabase(Host, UserName, Password)
.
Work with database
.
```

source1.vbs

```
.
.
UserName = “app”
Password = PVToolKit(“Vault.ini”,“User.ini”,“Safe”,“Root\Password”)
Host = “10.10.3.56”
ConnectDatabase(Host, UserName, Password)
.
Work with database
.
```

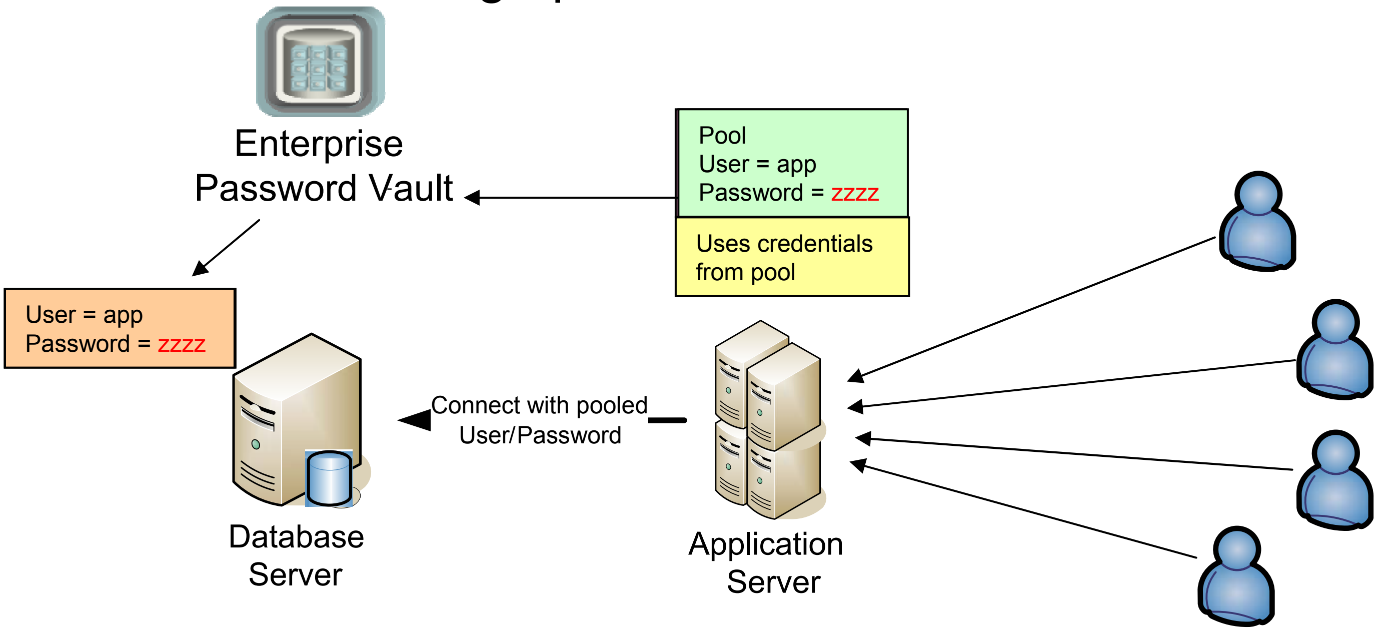
source1-new.vbs

The Problem

- Data sources credentials are stored in XML files
  - Hard to manage credentials
    - Leads to weaker credentials
    - Credentials are shared among IT and development users
    - Regulation and compliance issues
  - XML files may not be protected
  - No audit on password usage

Application Servers – cont.

- Password change process



- Application Server accesses the EPV whenever a password is required
- Caching is available in Agent running of the Application Server machine

Une solution éprouvée

Deloitte & Touche

PCAOB®
Public Company Accounting Oversight Board

CENDANT

citigroup

ABN·AMRO

LEHMAN BROTHERS

The Gillette Company

ING DIRECT

NOVARTIS

Roche

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
National Institutes of Health

MOTOROLA
intelligence everywhere™

Lucent Technologies
Bell Labs Innovations

WELLS FARGO

belgacom

Virgin money

AstraZeneca

Pfizer

Final Word from IDC

The risk of internal data misuse can be significantly mitigated by implementing policies that demand special treatment for privileged passwords…

There should be corporate mandates that privileged passwords be changed/reset routinely and on a system wide basis….

These types of actions constitute a best-practices approach to PPM, an important component of a sound overall IAM system implementation……

www.cortina.fr

Cortina La protection de vos informations est notre coeur de métier

Security – Down The Pan?

Transcription de l'article[1] signé Calum MacLeod, paru le 10th November 2004 dans *IT Backbones The Security News*,

They say that travel broadens the mind, and I have recently discovered a new phenomenon – the Secure Toilet.

On a recent trip to Switzerland, I visited a restaurant that secures the toilets with a digital lock. Both the ladies and the gents have a key-pad on the door, and with the right combination you can enter. Now this shouldn't come as a surprise given our heightened security awareness these days, and that the Swiss are obviously very security conscious, and every restaurant proprietor will tell you that misuse of toilet facilities is an increasing problem – It must be otherwise why secure then with digital locks.

Of course this security feature raises new problems.

For example you don't want your clientele rushing to the toilet only to discover that they can't get in because they don't know the combination. This will just create all sorts of complaints. But the Swiss have addressed this problem by placing signs all around the restaurant that refer you to the "WC Code", with instructions to ask a member of staff for the code. So far so good, but as you can appreciate the staff have more than enough on their plate than to spend all day keeping track of the code, and here's where the system starts to fail.

"You would be amazed at the number of organisations that use one password for hundreds of embedded accounts"

When I sat down in the restaurant I was facing the door into the kitchen and the first thing that caught my eye was a notice board, just where the staff entered the kitchen, with the inscription "WC Code 1213". Further investigation – I asked the waiter – revealed that the code is changed every night, and that the same code is used for the ladies and the gents, possibly to avoid embarrassing situations.

What is the point you might ask? Well if anything illustrates the problem of privileged access control – after all the toilets are for privileged users – customers – it's the secure toilet.

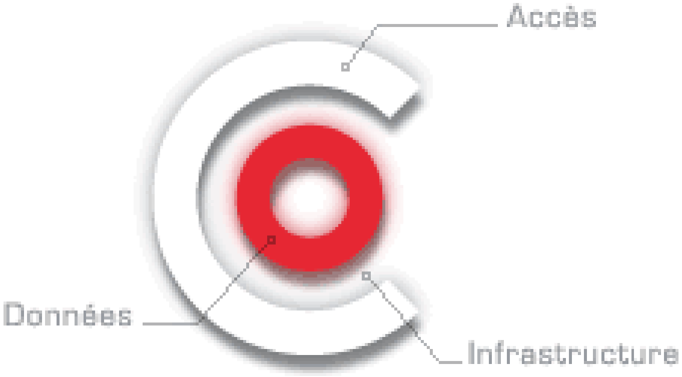
In the same way that the restaurant doesn't simply want people walking in off the street using the toilets, companies can't simply allow anyone to access privileged accounts or information in their organisation. And since it is not possible to provide access based on user identity, some mechanism has to be put in place to control this. So in the same way as the restaurant introduced the WC Code procedure, many companies talk about "Emergency Envelopes", or "Break Glass" accounts. The concept is the same – since you can't identify the user since they are called "administrator" or "root", or some other manufacturer embedded account, you protect the password.

This concept is fine on paper (and usually that's where the passwords are) but in practice it doesn't work. If you compare it to the toilet analogy, security staff have to follow similar procedures. Firstly someone has to manually change the password on a regular basis. One or two toilets are fine, but if we're n about every toilet in the city or in the now need an army to do this. The with passwords for embedded a someone has to change these manua

Now the next to ensure that changing the don't simply same passwor the place understand getting – If code to one got them all – with the pass would be amazed at the n organisations that use one pas hundreds of embedded accounts, f all domain passwords may be the s root passwords on every Unix se same, or all Oracle database accounts are the same. Now it complex code which no hacker in could figure out, but since it's so co probably means that I have to wri

[1] http://www.theitshield.com/pr/3489

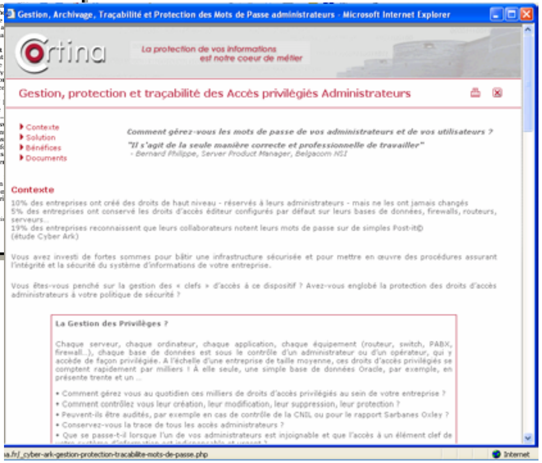
CORTINA – Siège: 14 avenue Jean-Baptiste Clément, 92100 Boulogne-Billancourt – Tél: 01 41 10 26 10 – info@corti
www.cortina.fr



Accès

Données

Infrastructure



Gestion, Archivage, Traçabilité et Protection des Mots de Passe administrateurs - Microsoft Internet Explorer

Cortina La protection de vos informations est notre coeur de métier

Gestion, protection et traçabilité des Accès privilégiés Administrateurs

- Contexte
- Solution
- Bénéfices
- Documents

Comment gérez-vous les mots de passe de vos administrateurs et de vos utilisateurs ?

"Il s'agit de la seule manière correcte et professionnelle de travailler"
- Bernard Philippe, Server Product Manager, Belgacom NSI

Contexte

10% des entreprises ont créé des droits de haut niveau - réservés à leurs administrateurs - mais ne les ont jamais changés
5% des entreprises ont conservé les droits d'accès éditeur configurés par défaut sur leurs bases de données, firewalls, routeurs, serveurs...
19% des entreprises reconnaissent que leurs collaborateurs notent leurs mots de passe sur de simples Post-it©
(étude Cyber Ark)

Vous avez investi de fortes sommes pour bâtir une infrastructure sécurisée et pour mettre en œuvre des procédures assurant l'intégrité et la sécurité du système d'informations de votre entreprise.

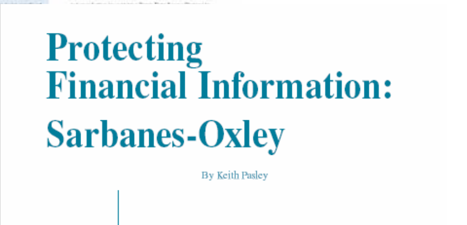
Vous êtes-vous penché sur la gestion des « clefs » d'accès à ce dispositif ? Avez-vous englobé la protection des droits d'accès administrateurs à votre politique de sécurité ?

La Gestion des Privilèges ?

Chaque serveur, chaque ordinateur, chaque application, chaque équipement (routeur, switch, PABX, firewall...), chaque base de données est sous le contrôle d'un administrateur ou d'un opérateur, qui y accède de façon privilégiée. A l'échelle d'une entreprise de taille moyenne, ces droits d'accès privilégiés se comptent rapidement par milliers ! À elle seule, une simple base de données Oracle, par exemple, en présente trente et un ...

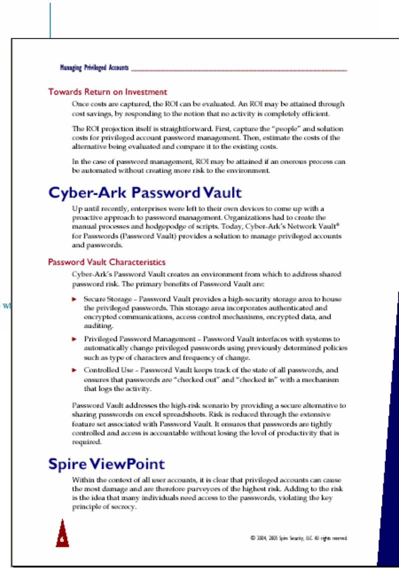
- Comment gérez vous au quotidien ces milliers de droits d'accès privilégiés au sein de votre entreprise ?
- Comment contrôlez vous leur création, leur modification, leur suppression, leur protection ?
- Peuvent-ils être audités, par exemple en cas de contrôle de la CNIL ou pour le rapport Sarbanes Oxley ?
- Conservez-vous la trace de tous les accès administrateurs ?
- Que se passe-t-il lorsque l'un de vos administrateurs est injoignable et que l'accès à un élément clef de

a.fr/_cyber-ark-gestion-protection-tracabilite-mots-de-passe.php
Internet



Protecting Financial Information: Sarbanes-Oxley

By Keith Pasley



Managing Privileged Accounts

Towards Return on Investment

Once costs are captured, the ROI can be evaluated. An ROI may be attained through cost savings, by responding to the notion that no activity is completely efficient.

The ROI projection itself is straightforward. First, capture the "people" and solution costs for privileged account password management. Then, estimate the costs of the alternative being evaluated and compare it to the existing costs.

In the case of password management, ROI may be attained if an onerous process can be automated without creating more risk to the environment.

Cyber-Ark Password Vault

Up until recently, enterprises were left to their own devices to come up with a proactive approach to password management. Organizations had to create the manual processes and hodgepodge of scripts. Today, Cyber-Ark's Network Vault® for Passwords (Password Vault) provides a solution to manage privileged accounts and passwords.

Password Vault Characteristics

Cyber-Ark's Password Vault creates an environment from which to address shared password risk. The primary benefits of Password Vault are:

- Secure Storage – Password Vault provides a high-security storage area to house the privileged passwords. This storage area incorporates authenticated and encrypted communications, access control mechanisms, encrypted data, and auditing.
- Privileged Password Management – Password Vault interfaces with systems to automatically change privileged passwords using previously determined policies such as type of characters and frequency of change.
- Controlled Use – Password Vault keeps track of the state of all passwords, and ensures that passwords are "checked out" and "checked in" with a mechanism that logs the activity.

Password Vault addresses the high-risk scenario by providing a secure alternative to sharing passwords on excel spreadsheets. Risk is reduced through the extensive feature set associated with Password Vault. It ensures that passwords are tightly controlled and access is accountable without losing the level of productivity that is required.

Spire ViewPoint

Within the context of all user accounts, it is clear that privileged accounts can cause the most damage and are therefore purveyors of the highest risk. Adding to the risk is the idea that many individuals need access to the passwords, violating the key principle of secrecy.

SOA Compliance W

Cortina

www.cortina.fr

Cyber-Ark