SearchFinancialSecurity.com INFORMATION SECURITY FINANCIAL INFORMATION SECURITY DECISIONS

Best Practices In Managing Privileged Access

June 2008

Andras Cser

Sr. Analyst, Forrester Research

FORRESTER®

Theme

Sharing access to sensitive accounts is inevitable, but poses security risks.

Adequate control can mean the difference between disasters and effective operations.

Agenda

- What is PUPM
- Why we need PUPM
- Best practices
- Today’s solutions
- Benefits of better management
- Market directions

Agenda

- What is PUPM
- Why we need PUPM
- Best practices
- Today’s solutions
- Benefits of better management
- Market directions

Definition: Privileged Accounts

- **Sensitive, often administrative accounts which are used by more than one person or system**
  - Administrative accounts and passwords are inherently shared by multiple people
    - Persistently or temporarily
    - In a controlled or uncontrolled way
  - UserIDs and passwords are hard-coded into apps

Why we have, and need, shared and privileged accounts

Admin accounts

- UNIX root
- DBAs
- Windows admins
- Network devices
- Legacy apps
- Security products
- Help Desk
- Fire drills
- Developer use

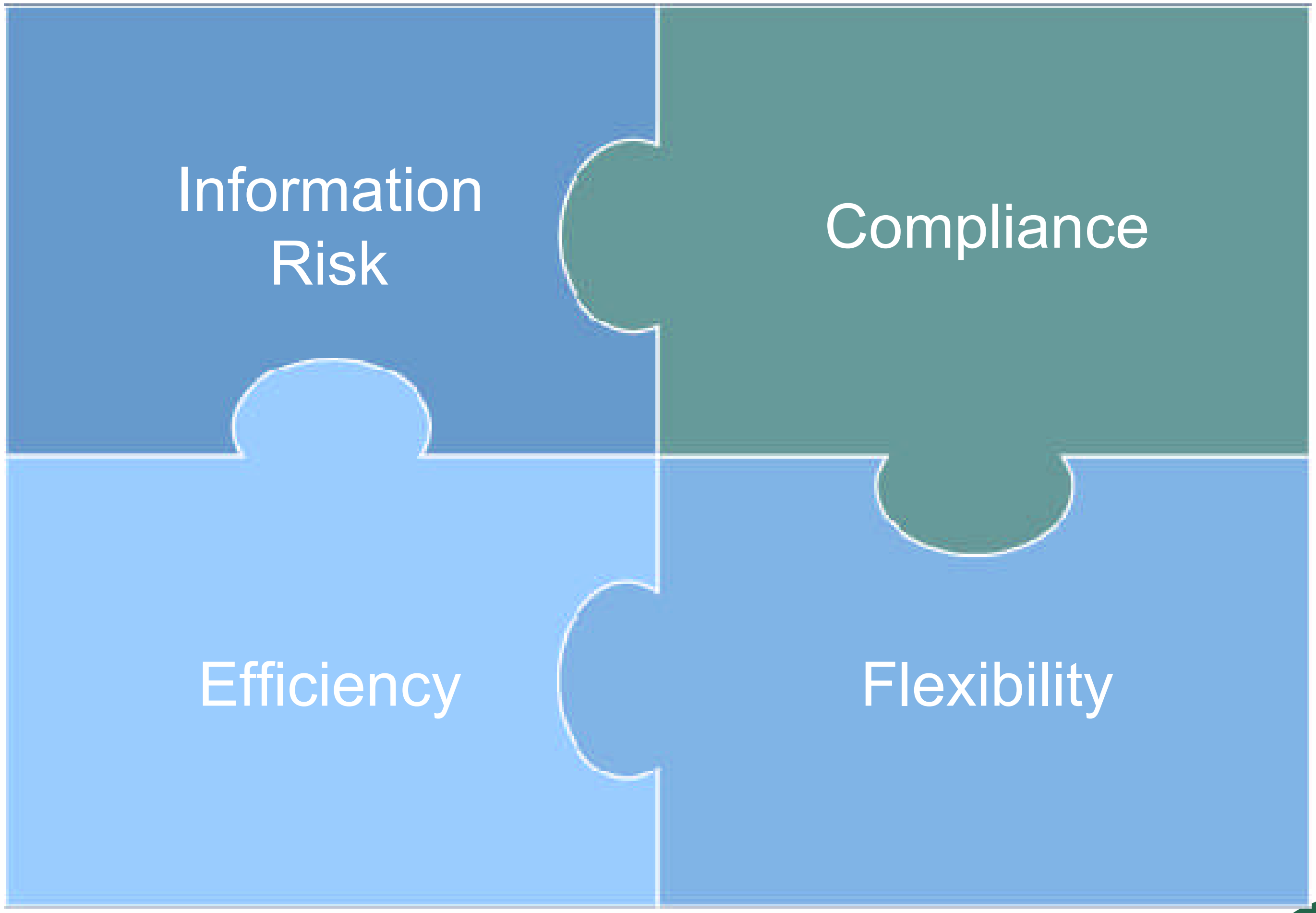
Application accounts

- Generic IDs
- Application IDs
- Batch jobs
- Test scripts
- Scheduled tasks

Individual accounts

- Assistant access while on vacation
- Limited time/use for Help Desk
- Pool of generic accounts for contractors

Why privileged and shared accounts are problematic



Information Risk

Compliance

Efficiency

Flexibility

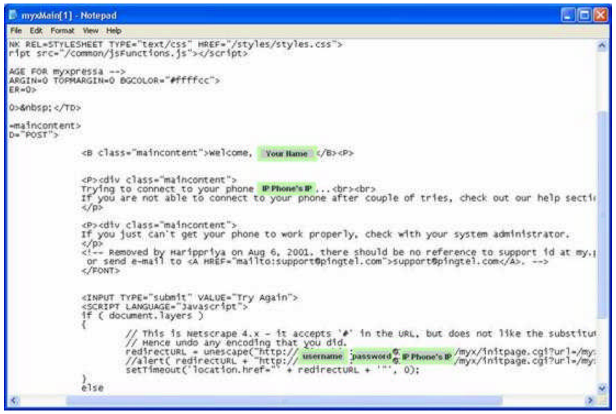
Agenda

- What is PUPM
- **Why we need PUPM**
- Best practices
- Today’s solutions
- Benefits of better management
- Market directions

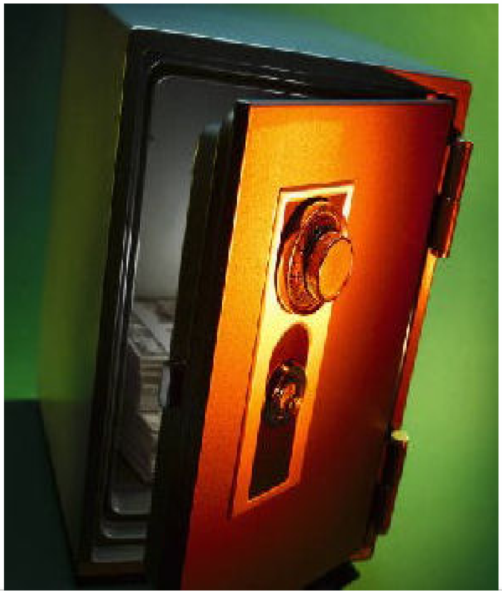
System administration scope is increasing…

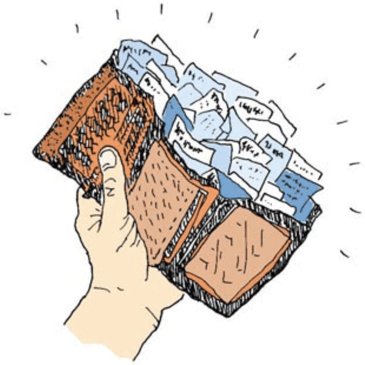
- To an ever increasing number of systems
- On an ever increasing number of platforms
- With more and more distributed staff
- On a global scale
- With extensive logging and auditing requirements

The old way of managing passwords does not work



```
NK REL=STYLESHEET TYPE="text/css" HREF="/styles/styles.css">
ript src="/common/jsFunctions.js"></script>

AGE FOR myxpressa -->
ARGIN=0 TOPMARGIN=0 BGCOLOR="#ffffcc">
ER=0>

O>&nbsp;</TD>

=maincontent>
D="POST">

          <B class="maincontent">Welcome, Your Name </B><P>

          <P><div class="maincontent">
          Trying to connect to your phone IP Phone's IP ...<br><br>
          If you are not able to connect to your phone after couple of tries, check out our help secti
          </p>

          <P><div class="maincontent">
          If you just can't get your phone to work properly, check with your system administrator.
          </p>
          <!-- Removed by Haripppriya on Aug 6, 2001. there should be no reference to support id at my.p
           or send e-mail to <A HREF="mailto:support@pingtel.com">support@pingtel.com</A>. -->
          </FONT>


          <INPUT TYPE="submit" VALUE="Try Again">
          <SCRIPT LANGUAGE="Javascript">
          if ( document.layers )
          {
                    // This is Netscrape 4.x - it accepts '#' in the URL, but does not like the substitu
                    // Hence undo any encoding that you did.
                    redirectURL = unescape("http://username:password@IP Phone's IP/myx/initpage.cgi?url=/my
                    //alert( redirectURL + "http://username:password@IP Phone's IP/myx/initpage.cgi?url=/my
                    setTimeout('location.href="' + redirectURL + '"', 0);
          }
          else
```





Typical audit findings that PUPM can remediate

- **Insufficient visibility into who accessed what system with elevated privileges**
- **No change log for network equipment configuration**
- **Approval of system administration is nonexistent**
- **Fire-call procedures are ad-hoc**
- **Administration is outsourced without proper controls**
- **Sensitive passwords are stored in configuration files**
- **SDLC issues with configuration migration**

Auditing of privileged access is essential…

- Auditors get smarter every year
- Audit findings get more expensive to fix
- Need to audit password change history, password complexity, checkout, and check-in of passwords
- Application to application access is gaining importance

Agenda

- What is PUPM
- Why we need PUPM
- **Best practices**
- Today’s solutions
- Benefits of better management
- Market directions

Best practices — People

- **Expect organizational resistance**
- **Prove the value of PUPM by tracking metrics**
  - Time it takes for an administrator to gain access in a production outage
  - Approval times
  - Cost of remediating audit findings
- **Develop a marketing and training/awareness plan for PUPM**
- **Involve application developers for the application to application passwords**

Best practices — Process

- Document PUPM process
- Review and document all AS-IS sources of passwords
- Review and document all AS-IS procedures for firecall activity, especially in production
- Understand and quantify risk of mismanagement/unauthorized management of systems
- Review grouping of systems quarterly
- Review minimum levels of system administrator permissions and adjust where needed
- Augment identity audits with PUPM audits

Best practices — Technology

- Use a renowned PUPM vendor’s solution
- Tally existing programming languages in app2app passwords
- Appliance based or software only solution
- Backup the safe periodically
- Find out from vendor if emergency export of the safe is possible in cleartext
- Integrate with an IAM (identity and access management) solution
- Integrate with a SIEM solution

Agenda

- What is PUPM
- Why we need PUPM
- Best practices
- **Today’s solutions**
- Benefits of better management
- Market directions

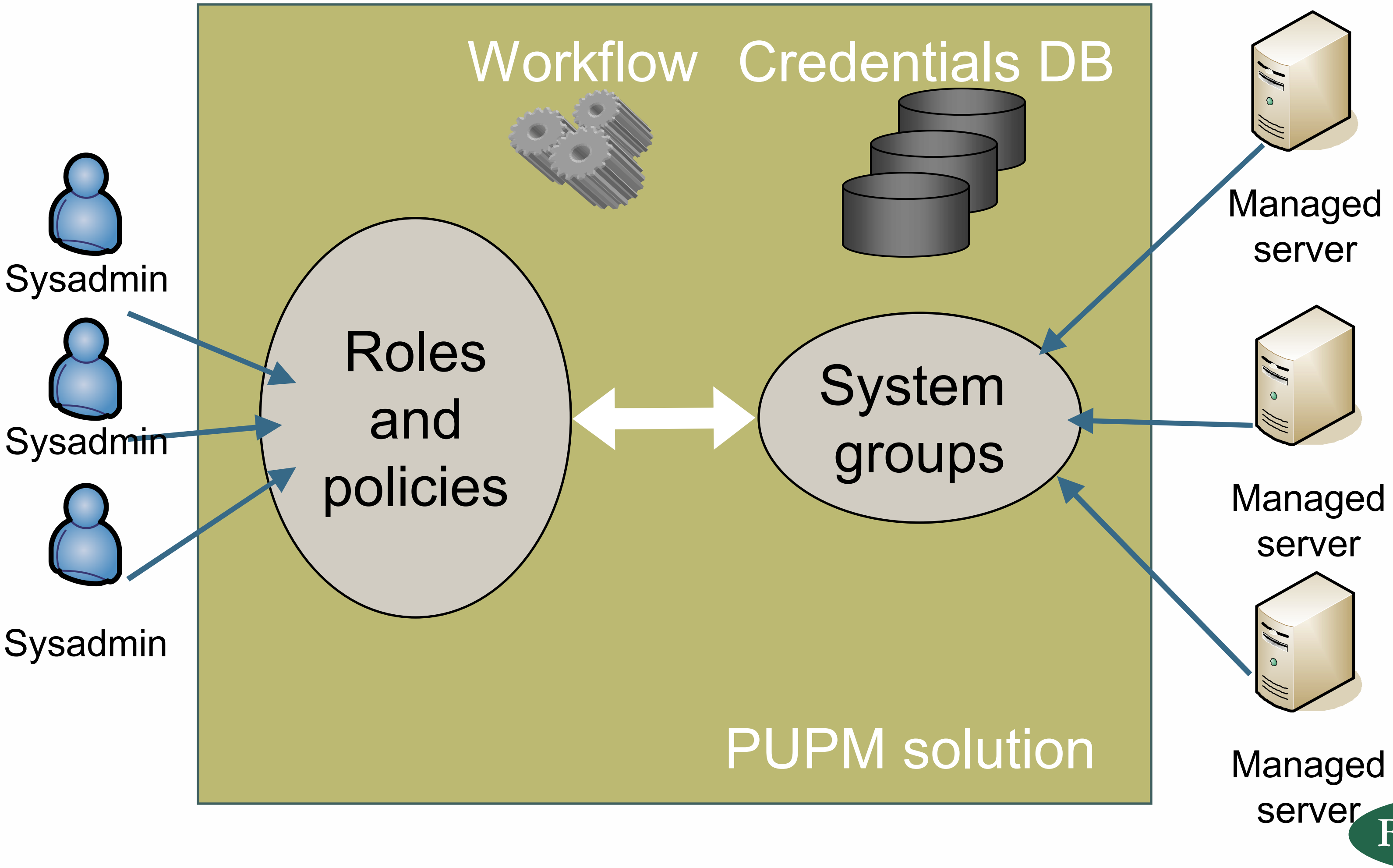
Today's solutions

- **Secure and central storage of passwords**
- **Automated and time-based password change and verification**
- **Provide policies and workflows for**
  - Approvals
  - Password checkout/check-in
  - Allowed use
- **Role based access**
- **Workflow**

Common features

- **Extensive audit**
- **Tamper resistant**
  - Passwords
  - Logs
- **Limited integration with provisioning/IAM solutions**
- **Appliance or software only form factor**

High level architecture



Workflow

Credentials DB

Sysadmin

Sysadmin

Sysadmin

Roles and policies

System groups

Managed server

Managed server

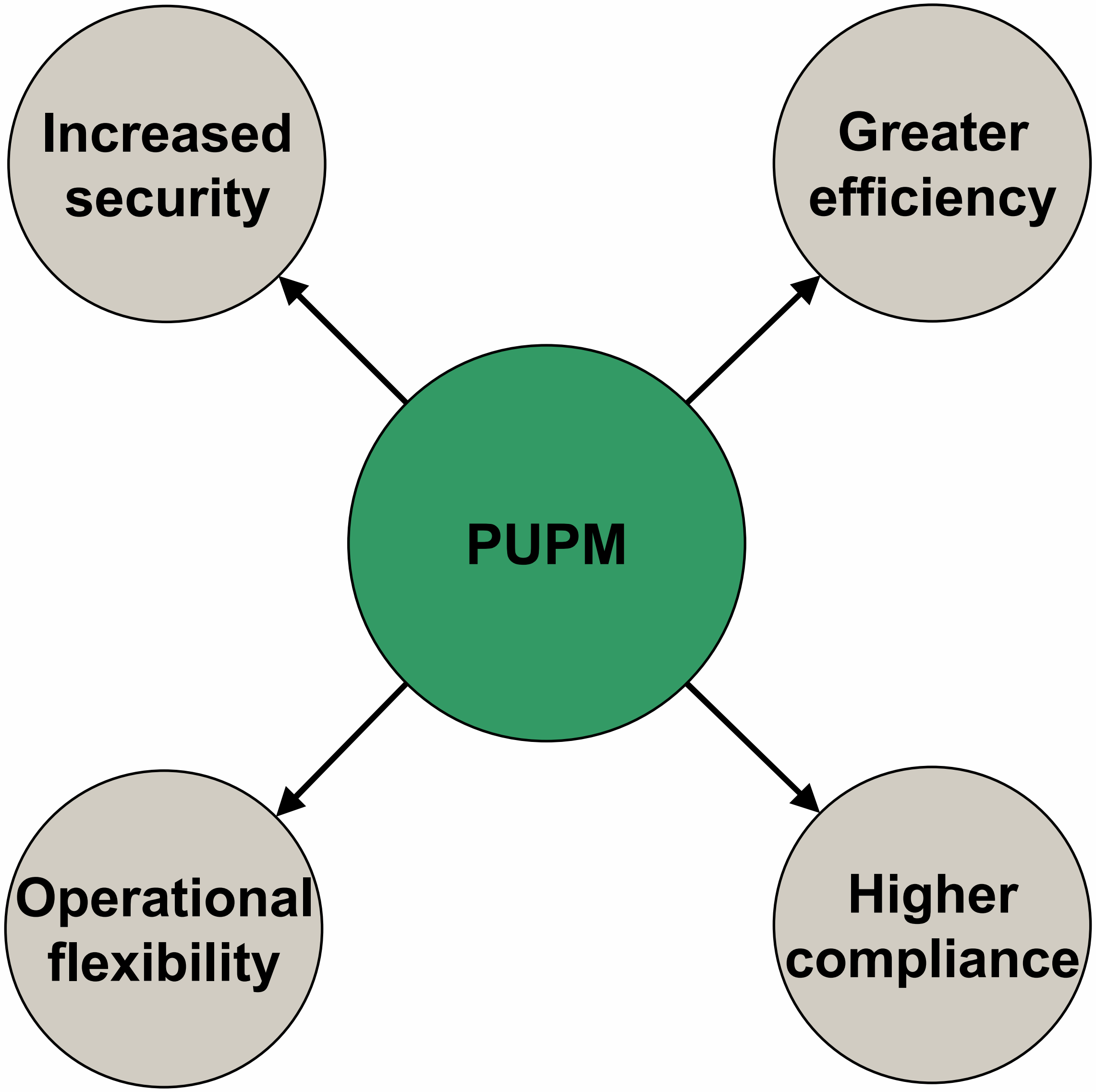
Managed server

PUPM solution

Agenda

- What is PUPM
- Why we need PUPM
- Best practices
- Today’s solutions
- **Benefits of better management**
- Market directions

Benefits of better management



Agenda

- What is PUPM
- Why we need PUPM
- Best practices
- Today’s solutions
- Benefits of better management
- **Market directions**

Market directions for PUPM

- Integration with enterprise single sign-on (eSSO)
- Auditing of finer grained actions
- Productivity improvements
- Increased support for strong AuthN
- Broader and richer target systems support
- Mobile device support
- Minimally invasive application to application password support

Vendor comparison

Vendor Feature	Cloakware	Cyber-Ark	eDMZ	Lieberman	Symark
Hardware/Software	Both	Both	HW	Both	HW
Market presence	Low	High	High	High	Medium
New customers in 2007	Low	High	High	Medium	Low
Focus on PUPM	Low	High	High	High	Medium
Nested groups	Yes	No	Yes	Yes	No
Auto-detection of endpoints	No	Yes	No	Yes	No
Automatic sessions/hide password	No	Yes	Yes	No (beta version only)	Limited, CLI only
Strong AuthN	Yes	Yes	Yes	Yes	Yes
App2App password	Full	Full	Limited	Limited	None
Product callable in Web Services	None	None	None	WSE 3.0	None
Application to application passwords	Full	Full	Limited	Limited (ERPM only)	None

Thank you

Andras Cser

+1 617/613-6365

acser@forrester.com

Please visit www.forrester.com/fisd for a copy of this presentation and free complementary research from Forrester.