Best Practices In Managing Privileged Access

June 2008
Andras Cser
Sr. Analyst, Forrester Research
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

<table>
<thead>
<tr>
<th>Admin accounts</th>
<th>Application accounts</th>
<th>Individual accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• UNIX root</td>
<td>• Generic IDs</td>
<td>• Assistant access while on vacation</td>
</tr>
<tr>
<td>• DBAs</td>
<td>• Application IDs</td>
<td>• Limited time/use for Help Desk</td>
</tr>
<tr>
<td>• Windows admins</td>
<td>• Batch jobs</td>
<td>• Pool of generic accounts for contractors</td>
</tr>
<tr>
<td>• Network devices</td>
<td>• Test scripts</td>
<td></td>
</tr>
<tr>
<td>• Legacy apps</td>
<td>• Scheduled tasks</td>
<td></td>
</tr>
<tr>
<td>• Security products</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Help Desk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Fire drills</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Developer use</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
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

Roles and policies

System groups

Managed server

Workflow

Credentials DB

Sysadmin

PUPM solution

Sysadmin

Sysadmin

Managed server

Managed server

Managed server
Agenda

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

- Increased security
- Greater efficiency
- Operational flexibility
- Higher compliance

PUPM
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

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