Cyber-Ark Software: how to select a Password Management System

Cyber-Ark Software: how to select a Password Management System. Sometimes when I look at envelopes I understand technology. When I was a student in college, I worked in the server room where we had a secret lock box full of envelopes. Every time I had to upgrade a database or create a new user, I remember looking for the right envelope (will it be this yellow one? Will it be this blue one?). After I found it, I went happily to the designated server. You can imagine how disappointed I was when I went to the Windows server or to the Unix server, typed the password stored in the envelope and got “Username and password do not match” or “The system could not log you on. Make sure your user name and domain are correct.” Imagine yourself on a cold night, all you want to do is finish this shift and you can’t. Just because someone forgot to update the password in the envelope!

In another company where I worked, we didn’t have envelopes. However, any employee who had worked there during the previous four to five years could come whenever he wanted (and I mean any year that he wanted...) and type the “standard” password – Passw0rd? The name of the company? Top secret? Admin? Q1w2e3? And like magic, they were in with the most powerful permissions.

Standard passwords become widely known to every worker, vendor or technician who visits your company; I assume in your private house you wouldn’t let this happen, would you? Well, in a world where we don’t have extra time and everything is automatic, why should we waste time managing administrative passwords manually?

What Should You Look for in a Password Management System?

You Want It to Be Safe and Secure

These are the most powerful passwords in the organisation; you don’t want them stored in an Excel file or in an Access database. Just imagine what could happen if someone accessed the local administrator password for the Active Directory or the Web server?
Full Integration with your Organisation

Many companies can write a nice application to store passwords in an Access database, but you need much more than this.

For example:

- Backup integration (Veritas, Backup exec...);
- monitor integration (Hp openview, Tivoli);
- transparent user management (LDAP integration) (user’s point of view) – you don’t want to redefine all the IT department users again.
- Automatic synchronisation – machines are added and removed from the network on a daily basis. You want a system that can automatically reflect these changes.

“Two clicks to a password” Web Interface

In the end, your IT department will need to use these administrative passwords quite often; it should be easy for them to access them.

Full Audit

You, as a manager, want to know exactly who used the last root password. Who used the administrative password of the CEO laptop, who took the emergency password of the Mainframe? You must comply with regulations and you should ask for state-of-the-art security software that will store the audit trails.

Disaster Recovery

You are going to store keys to your most sensitive and important data; you had better have a robust disaster recovery component.
Automatic Change of Passwords

Regulations force you to change your passwords every 30 days. This means the end of the manual era. You need the Password Management System to change the local administrator passwords on the 10,000 desktops that you have as well as the entire set of Unix servers root passwords. Of course you don’t want to install any agents on the servers and desktop, do you?

In addition, I recommend this list of devices as a comprehensive list of supported platforms that Password Management Systems should support: Microsoft Windows XP, Microsoft Vista, Windows 2000, 2003 (local and domain), IBM AIX, IBM OS/400, IBM OS/390 (RACF), Sun Solaris, HP HPUX, Microsoft Windows Services, Scheduled Tasks, Oracle Database, Microsoft SQL Server, IBM DB2, IBM Informix, Sybase Database, MySQL, Any ODBC compliant database, Checkpoint FW-1, Nokia Checkpoint FW-1 on IPSO, Cisco PIX, Juniper Netscreen, FortiGate (web content filtering), Cisco Router, Cisco Switch (Catalyst), Juniper Router (Junos), Alcatel Switch (Omniswitch 7000 Series), Quintum VOIP, F5 BigIP, Microsoft Active Directory, Unix Kerberos and NIS Directories and Credential Storage, IBM HMC, Sun ALOM, Digi Console Management (CM), IBM Websphere.

High Availability

As we said in previous sections, we are dealing with the most sensitive passwords in your organisation. You want the Password Management System to provide maximum availability to the enterprise and assure business continuity.

Management Dashboard

You, as a manager, should be able to see a real-time snapshot of administrative passwords and privileged account usage. The dashboard should include a group of different charts that graphically display your compliance with policies, usage status and, of course, anomaly activities.

Hard Coded Passwords

Many scripts contain hard coded passwords. These scripts are not secured and they contain the password in plain text. Any “new employee” can look at these scripts and take the passwords to “explore their limits”. You need a component in the Password Management System that will solve this problem and will integrate easily with your application server.

Distributed Architecture
You probably have more than two network areas, so your Password Management System should have centralized management with the ability to change passwords on a distributed network, without needing to redesign your entire network structure.

**Proven Enterprise Class Scalability**

Check that enterprises like yours are fully satisfied with their chosen solution. The above elements will help you know what to look out for when you embark on rolling out a successful Password Management System.

Nowadays it’s is key for all enterprises to make sure that data is kept safe and secure at all times. After all, there’s a lot of money in the sale of sensitive data which staff internally and externally frequently trade in – so it’s imperative that you know how to keep it under virtual lock and key!

Contact:

**Oded Valin**
Cyber-Ark Software,  
Eindhoven, The Netherlands  
info@cyber-ark.com  
www.cyber-ark.com