AUTOMATE YOUR VULNERABILITY AND COMPLIANCE AUDITS WITHOUT LEAVING YOUR PRIVILEGED ACCOUNTS VULNERABLE TO ATTACK.

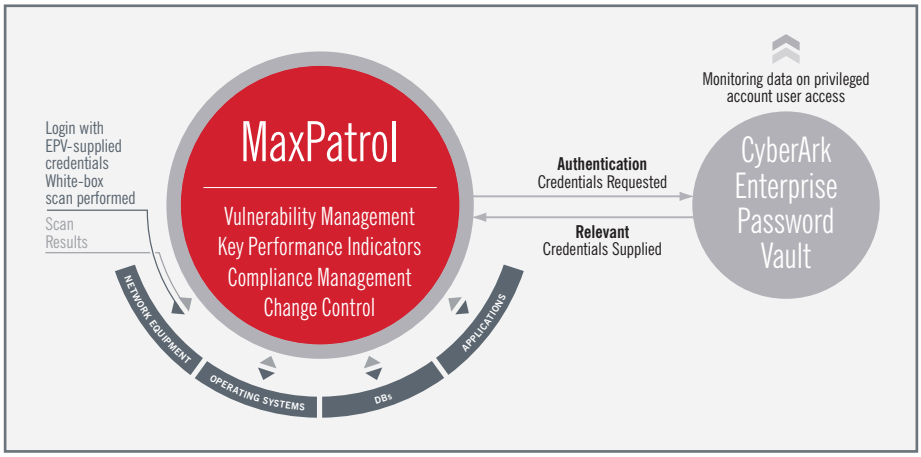

Figure 1. CyberArk EPV and MaxPatrol integration

Highlights

+ Assure your privileged accounts are protected and your network systems are safe and compliant
+ Save time and money while increasing your security with a fully automated solution
+ Leverage the power of both MaxPatrol and Enterprise Password Vault — at the click of a button

THE CHALLENGE

Privileged identity management is an essential part of enterprise security – protecting thousands of accounts on critical systems from brute force attacks and hackers who can easily guess default IDs and weak passwords. Identity management solutions solve this problem by frequently rotating user credentials for these privileged accounts; but in the process break another key part of your IT Security armour – vulnerability and compliance management (VCM).

Remaining constantly aware is also vital when you're monitoring security compliance or checking for new vulnerabilities. For that reason, it is wise to select a VCM solution that automatically performs regular scans of your entire network to find areas where you fail to meet the relevant standards and to detect weaknesses that leave you vulnerable to attack. But to perform a complete analysis, a VCM solution must be logged-in to the system it is scanning. And that's where the dilemma arises: how can an automated VCM solution know which privileged credentials to use if an identity management system is continuously changing them for security reasons?

THE SOLUTION:

MaxPatrol and CyberArk Enterprise Password Vault

CyberArk's Enterprise Password Vault allows organizations to enforce password policies across their privileged accounts. It generates long, complex passwords which are known only to CyberArk Enterprise Password Vault and the target system. Passwords are updated automatically at pre-determined intervals. CyberArk Enterprise Password Vault securely stores credentials for all target systems and shares them with authorized users or third party solutions, like MaxPatrol, only when they are required.

The MaxPatrol vulnerability and compliance management solution employs advanced white-box security analysis to give enterprises regular, automated assessments of their compliance levels with a wide range of global security standards such as ISO, PCI DSS

continued

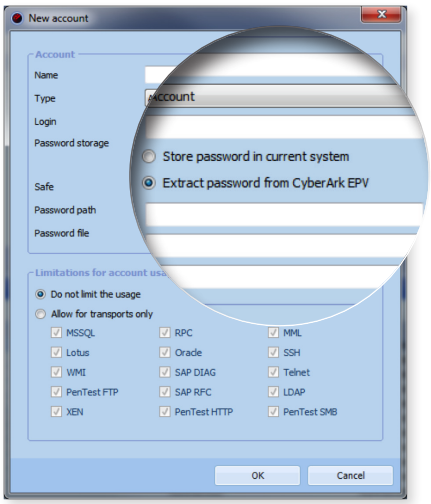

Figure 2. Configuration screen for CyberArk Enterprise Password Vault account access within MaxPatrol administration console

and SOX as well as regional requirements and internal corporate policies. When armed with privileged access, MaxPatrol generates a complete inventory of systems and applications, checks compliance and scans for vulnerabilities that leave them at risk of attack.

Positive Technologies has integrated MaxPatrol with CyberArk Enterprise Password Vault to ensure it can seamlessly acquire the privileged identities from the CyberArk solution that it needs to perform security assessments. By simply selecting the CyberArk Enterprise Password Vault option in MaxPatrol's admin console, you can authorize MaxPatrol to obtain protected credentials for each system just before it begins an audit. Privileged account details are stored in MaxPatrol only for the length of time specified by CyberArk Enterprise Password Vault; maintaining the solution as the single repository for securing user details – giving you the confidence that IDs won't leak outside your organization, even to your most trusted partners. For auditing purposes, CyberArk Enterprise Password Vault makes a record every time MaxPatrol uses a privileged credential.

The combination of MaxPatrol and CyberArk Enterprise Password Vault provides you with the automated vulnerability and compliance management and control of privileged accounts you need to secure your assets and protect your business.

About CyberArk

CyberArk is trusted by many of the world's leading companies, including 40 of the Fortune 100, to protect their highest-value information assets, infrastructure and applications. For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. With offices in the US, Israel, UK, France, Germany, Netherlands and Singapore, CyberArk serves more than 1,400 global business in 55 countries. These customers include 17 of the world's top 20 banks, eight of the world's top 12 pharmaceutical firms and 75 leading energy companies. **www.cyberark.com**

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

CYBER_PAB_A4.ENG.0007.01.DEC.29.2014