epas

Enterprise Password Assessment Solution

The Future of Password Security is Here

EPAS – Enterprise Password Assessment Solution

The number one risk of any IT security architecture, no matter how thorough and extensive, remains the human factor – mainly the way users interact with the IT environment through the use of passwords. A number of effective measures can be taken to secure an IT security infrastructure, for example antivirus programs, firewalls or the implementation of encryption. Weak passwords in the authentication process still pose an unpredictably high risk. And this is what attackers will target.

60 % or more of passwords used in companies do not satisfy minimum security requirements.

EPAS is a solution developed by Detack GmbH and its Swiss partner Praetors AG. It is an on-premises SaaS solution for enterprise wide, automatic and regular password quality assessment and enforcement for a wide range of systems. EPAS addresses the overwhelming issue of maintaining secure passwords in large, heterogeneous environments containing Microsoft A/D, IBM System z, SAP and more. EPAS uses a self-developed, patent pending technology designed for enterprises, to extract all relevant password data from a target system, and uses these to assess the resilience of passwords against attacks. EPAS employs only legitimate cipher text extraction methods and therefore creates no system stability risk for the target.

Password Strength

Password policies commonly enforce length and composition requirements. Their effectiveness against current password recovery attacks has been proven to be very low. Attackers use many different methods in the attempt to compromise a password, the most common being the dictionary attack. Millions of words - from dictionaries, literature and passwords from internet password leaks – are used to create millions of password hashes. These hashes are then compared to those saved on a company server. A policy does not restrict the use of dictionary words and known derivations, i.e. substituting the @-symbol for an "a". The true strength of a password – its resilience against attacks – can best be evaluated using structural entropy.

Universal Password Assessment

EPAS analyses the objective strength of passwords in selected target systems. Weak passwords are vulnerable to malicious cyber-attacks. EPAS is able to assess unsalted, statically salted, as well as dynamically salted passwords. It is customized for system specific encryption and evaluates personal, as well as technical and system accounts.

Detailed and Legally Compliant Reporting

EPAS generates audit reports for each audit job. An executive summary provides full text and graphical data to visualize and explain the passwords' overall quality. Included are recovery reasons, structure, compliance status and various other statistical data. Passwords are never displayed in clear text.

Built on 15 Years IT-Security Experience

EPAS was developed based on more than 15 years of IT-security auditing. The extensive experience of manual penetration tests sustainably shows that, without resilient passwords, all security measures are bound to fail. EPAS is unique and the only solution to offer a legally compliant view of your enterprise password landscape.
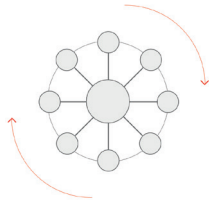
Designed for Enterprises

EPAS has been designed to meet the needs of modern enterprises. More than 30 different systems and databases, ranging from IBM, SAP, Oracle to Microsoft, are supported. Legally compliant reporting offers all security relevant password data whilst respecting the protection of personal data and satisfying workers councils´ requirements.
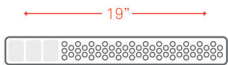
Customizable Password Assessment

EPAS audits the recovered passwords against two criteria: a customized password policy and an objective, entropy-based set of rule. EPAS can simulate various attack methods used by cyber criminals, such as dictionary or brute force attacks. Dictionaries are customizable regarding language and customer specific vocabulary or terms.
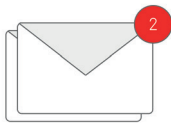
Password Re-Use Report

Recovered passwords are checked for multiple use. A password can either be used several times by the same user on different systems or one password can be used by several users. Both situations pose a high security risk and are subject to immediate risk mitigation measurements.
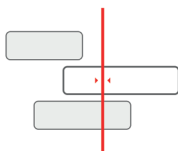
Technical and System Accounts

In addition to "heartbeat" users, all technical and system accounts are assessed and evaluated by EPAS. These accounts authenticate by using either very simple passwords, default vendor passwords, or no password at all. Yet these accounts usually have the highest privileges and are sometimes even exempt from a password policy. The authentication of technical and system accounts to other systems is one of the largest IT security risks.

Notification by E-Mail

Automatic notification is used to prompt users to change their passwords if these are too weak or do otherwise not comply with defined audit parameters. The same feature automatically notifies the service administrator of a completed password audit job and the availability of a report.

Audit Jobs & Job Queuing

An intelligent job and queuing system permits programmable, regular password auditing with no job collisions. EPAS is highly scalable. It can process simultaneous parallel tasks and can audit millions of accounts on different systems over a single weekend.

Trusted Computing and Encryption

All data EPAS processes is permanently encrypted. Trusted Computing is used to seal the platform, an additional TPM chip secures software and data integrity by employing cryptographic methods. EPAS applies various hardware and software monitoring elements to detect physical or software intrusion attempts. Security failsafe mechanisms log events and shut down in case of intrusion attempts.

On-Premises SaaS

EPAS is an on-premises SaaS solution and delivered through appliances which are integrated into the client´s data center. It is a "subscription-based service", meaning all hardware remains the property of the service provider at all times. Software updates and hardware upgrades are included in the yearly subscription fee.

Supported Standard Target Systems

Microsoft Active Directory Accounts
Microsoft Windows Local Accounts
IBM System z - zSeries - S/390 RACF (z/OS, z/VM)
IBM System i - iSeries - AS/400
IBM System p - pSeries - RS/6000 AIX
IBM Lotus Domino Application Server
BSD Operating System
Linux Operating System
Sun Solaris – SunOS
Apache Basic - htpasswd
SAP NetWeaver - ABAP AS
LDAP Authentication Server

Supported Application Specific Data Storage

MSSQL System Accounts
MySQL System Accounts
Oracle System Accounts
PostgreSQL System Accounts
Sybase ASE System Accounts
DB2 Database Custom Application
Informix Database Custom Application
MaxDB Database Custom Application
MSSQL Custom Database Application
MySQL Database Custom Application
Oracle Database Custom Application
PostgreSQL Custom Database Application
Sybase ASA Database Custom Application
Sybase ASE Database Custom Application

" *EPAS has helped us to increase our password security tremendously – a security problem we knew about and had to solve, but before had no means to truly control or monitor.*"

- A LEADING INTERNATIONAL INSURANCE COMPANY