epas

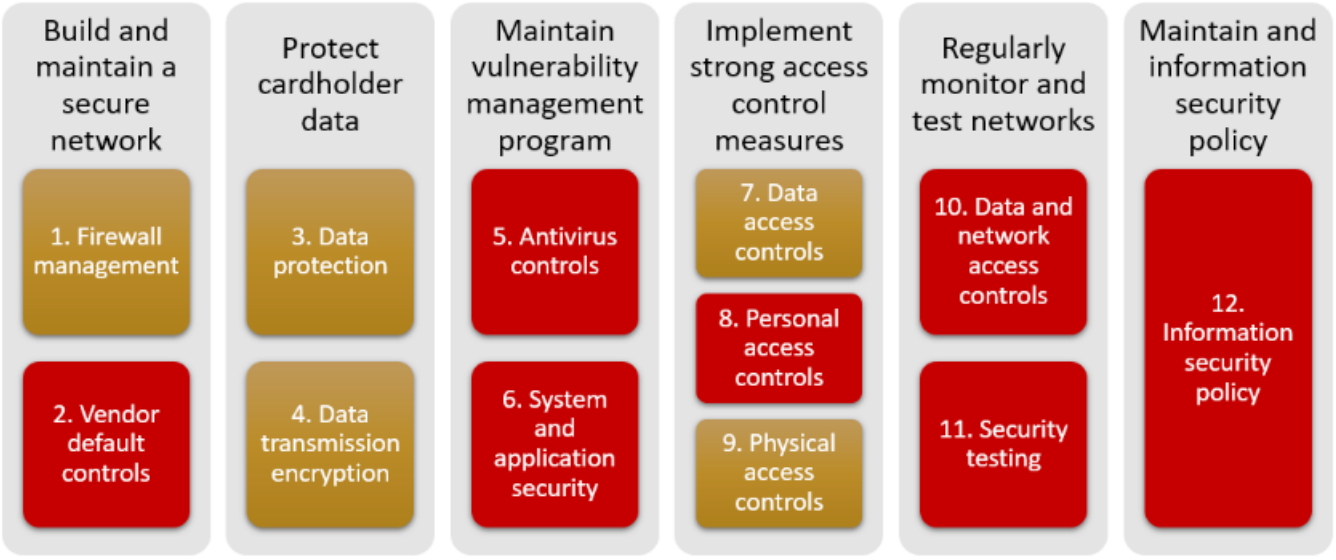
Enterprise Password Analytics Solution

EPAS for Compliance: PCI DSS

The PCI DSS security standard

The Payment Card Industry (PCI) initiated the first Data Security Standard (DSS) in 2004. Various revisions and updates have been done to the requirements since then. The PCI DSS contains twelve requirements for compliance, clustered by six logically connected controlled objectives.

„The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).“[1] In the following figure, there are presented the 12 PCI DSS requirements, having highlighted the ones which EPAS addresses.



■ Requirements that EPAS helps satisfying

1 Payment Card Industry (PCI) Data Security Standard, v3.2.1, © 2006-2018 PCI Security Standards Council.

Scope of PCI DSS

„The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is composed of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications."[1]

„The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and fail-over systems."[1]

EPAS mapping over PCI DSS requirements

PCI DSS standard provides the bare minimum requirements for protection against breaches which have occurred in the past. Therefore, it has a significant importance on the payment card ecosystem. EPAS strongly assists organizations preventing breaches based on several PCI DSS requirements, and especially one of the essential security rules of the standard, i.e. „To minimize the risk of being breached, businesses should change vendor default passwords to strong ones, and never share them – each employee should have its own login ID and password"[2]. Following, it is presented the EPAS mapping over PCI DSS requirements.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

- **Guidance**: „*Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.*"[1]

- EPAS Coverage:

  ✓ EPAS Audit analyses equipment and service accounts for the use of default passwords and provides data to enable remediation.

  ✓ EPAS Enforcer permits only compliant, non-default passwords to be used at the time of password change.

2 Payment Data Security Essential Strong Passwords: https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf

2.3 Encrypt all non-console administrative access using strong cryptography.

- Guidance: „*If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use.*"[1]

- EPAS Coverage:

✓ EPAS Audit identifies the cryptographic algorithms used to hash password data and reports the usage of weak cryptography or reversible encryption / clear text password storage.

2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

- Guidance: „*Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.*"[1]

- EPAS Coverage:

✓ Through EPAS Audit, equipment and service accounts are analysed for the use of default passwords and data is provided to enable remediation. This password management strategy is documented by the EPAS through an immutable audit trail.

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data.

- Guidance: „*This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients. This allows clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data.*

- EPAS Coverage:

✓ EPAS Audit identifies the usage of shared passwords, i.e. multiple tenants using the same authentication credentials.

✓ EPAS Enforcer prevents the usage of shared passwords. Even if this is not sufficient by itself to ensure tenant isolation, it is one of the mandatory controls.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

- **Guidance**: „*Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.*“[1]

- **EPAS Coverage:**

✓ EPAS Audit provides a policy quality assurance mechanism, offering a central view on password quality versus password policies, across heterogeneous and distributed environments. Management has a clear set of metrics based on which to implement controls and processes are in place to quality assure passwords.

✓ EPAS Enforcer provides granular and privacy compliant events whenever a password change occurs and whenever a password change fails due to password policy violations.

Requirement 6: Develop and maintain secure systems and applications.

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

- **Guidance**: „*The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment. Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds. Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information. Classifying the risks (for example, as “high,” “medium,” or “low”) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.*“[1]

- **EPAS Coverage:**

✓ EPAS Audit can identify the poor passwords used within an organisation, these representing a common vulnerability that can be exploited by an attacker. EPAS Audit also provides reports classifying the strength of a password.

✓ EPAS Enforcer prevents the use of weak, reused, or shared passwords whenever the password is changed.

6.3 Develop internal and external software applications (including web-based adminisrative access to applications) securely.

- Guidance: „*Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. Understanding how sensitive data is handled by the application—including when stored, transmitted, and when in memory—can help identify where data needs to be protected.*“[1]

- EPAS Coverage:

✓ Authentication security review is a mandatory element of any IT security test. Passwords are the most used authentication method. EPAS Audit analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication.

6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

- Guidance: „*Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.*“[1]

- EPAS Coverage:

✓ EPAS Audit provides a separate interface for voluntary password quality evaluation that is normally employed by users to check passwords before using them; this interface is also used in awareness training.

✓ EPAS Enforcer provides direct feedback on password strength during a password change, thus increasing awareness on security posture for all users.

Requirement 8: Identify and authenticate access to system components.

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.

- Guidance: „*By ensuring each user is uniquely identified— instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs. To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.*“[1]

- EPAS Coverage:

✓ EPAS Enforcer facilitates controlling the modification of a user‘s password and prevents the usage of shared passwords, that would prevent secure user identification.

✓ EPAS Audit identifies the gaps in the user identification mechanisms and provides remediation actions input.

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:
• Something you know, such as a password or passphrase
• Something you have, such as a token device or smart card
• Something you are, such as a biometric

- Guidance: *„These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for "something you have" as long as it is unique for a particular user. Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management."*[1]

- EPAS Coverage:

✓ Passwords are the most used authentication method. EPAS Audit is used to prove that the currently used passwords' quality level corresponds to the strong authentication requirements of relevant security policies and standards. EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication by using patented technology. It will detect and report clear-text passwords, passwords using reversible encryption, as well as passwords stored with weak / insecure hashing algorithms. The result is an authentication quality assurance mechanism, providing a central view on password quality versus password policies, across heterogeneous and distributed environments.

✓ EPAS Enforcer prevents weak access credentials, already exposed (leaked) passwords, as well as shared passwords. EPAS Enforcer provides direct feedback on password strength at password change. It is also used to define stricter policies to be enforced for privileged accounts.

8.4 Document and communicate authentication policies and procedures to all users including:
• Guidance on selecting strong authentication credentials
• Guidance for how users should protect their authentication credentials
• Instructions not to reuse previously used passwords
• Instructions to change passwords if there is any suspicion the password could be compromised.

- Guidance: *„Communicating password/authentication policies and procedures to all users helps those users understand and abide by the policies. For example, guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that don't contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access."*[1]

- EPAS Coverage:

✓ EPAS Audit supports organisations to directly address human-side risks by targeting tailored awareness and training to users, based on password audit reports. History of password audit results allow for training effectiveness measurement and escalating information and training for riskier users. EPAS Audit also provides an interface for voluntary password quality evaluation that is normally employed by users to check passwords before using them; this interface is also used in awareness training.

✓ EPAS Enforcer provides direct feedback on password strength at password change, thus increasing awareness on security posture for all users.

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:
• Generic user IDs are disabled or removed.
• Shared user IDs do not exist for system administration and other critical functions.
• Shared and generic user IDs are not used to administer any system components.

- Guidance: „*If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This, in turn, prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.*"[1]

- EPAS Coverage:

✓ EPAS Audit reports include detailed information about group and organizational unit membership, including nested groups. This enables fast identification of sensitive user rights, along with the password security metrics, for all accounts, including technical and accounts hard to identify. EPAS Audit will determine if passwords are shared amongst multiple users, and whether such passwords have been changed. EPAS Audit technology is used to both identify weak credentials that would expose secret information as well as shared credentials which would prevent accountability and would allow undetected data theft. EPAS Enforcer can prevent both weak access credentials as well as shared passwords. EPAS Audit allows defining stricter classes of password strength to be required for privileged accounts. Automatic notifications of violations and continuous metrics are used for provable strong authentication of privileged accounts.

✓ EPAS Enforcer is used to define stricter policies to be enforced for privileged accounts. For example, password reuse or password sharing can be blocked within the same system group or even across the entire organization.

8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

- Guidance: „*Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.*"[1]

- EPAS Coverage:

✓ EPAS Audit supports organisations to directly address human-side risks by targeting tailored awareness and training to users, based on password audit reports. History of password audit results allow for training effectiveness measurement and escalating information and training for riskier users. EPAS Audit also provides an interface for voluntary password quality evaluation that is normally employed by users to check passwords before using them; this interface is also used in awareness training.

✓ EPAS Enforcer offers direct feedback on password strength at password change, thus increasing awareness on security posture for all users.

Requirement 10: Track and monitor all access to network resources and cardholder data.

10.2 Implement automated audit trails.

- Guidance: „*Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities.*“[1]

- EPAS Coverage:

✓ EPAS Audit provides reports containing ongoing analytics that determine whether or not password policies need to be adapted to address the evolution of threats. Revision history on password rules can be followed in the EPAS management console. Referring to anti fraud, EPAS Audit provides a fine grained audit trail of passwords and password history. Evidence can be provided that a user was regularly prompted to improve their password.

10.5 Secure audit trails so they cannot be altered.

- Guidance: „*Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.*“[1]

- EPAS Coverage:

✓ The reports generated by EPAS Audit are stored into the same system where EPAS is running and can never be deleted, or altered, unless the administrator (usually, the security manager) chooses to delete them. The EPAS logs and audit trail cannot be deleted, even by administrators.

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

- Guidance: „*Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in offline locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.*“[1]

- EPAS Coverage:

✓ The reports generated by EPAS Audit are stored into the same system where EPAS is running and can never be deleted, or altered, unless the administrator (usually, the security manager) chooses to delete them. The EPAS logs and audit trail cannot be deleted, even by administrators.

Requirement 11: Regularly test security systems and processes.

11.3 Implement a methodology for penetration testing that includes the following:
• Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
• Includes coverage for the entire CDE perimeter and critical systems
• Includes testing from both inside and outside the network
• Includes testing to validate any segmentation and scope-reduction controls
• Defines application-layer penetration tests
• Defines network-layer penetration tests to include components that support network functions as well as operating systems
• Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
• Specifies retention of penetration testing results and remediation activities results.

- Guidance: „*The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities. Conducting a vulnerability scan may be one of the first steps a penetration tester will perform in order to plan the testing strategy, although it is not the only step. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way, a tester is able to simulate the methods performed by an attacker to identify areas of potential weakness in the environment.*“[1]

- EPAS Coverage:

✓ EPAS Audit analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system, fulfilling the privacy requirements of every policy. It also covers a wide range of critical systems (IBM systems, Microsoft A/D accounts, BDS OS, Linux OS, Apache Basic, LDAP authentication server, MySQL System Accounts, etc.) to be tested for the use of poor passwords. EPAS reports are fully stored within EPAS's hard drive as long as the solution belongs to the customer, if the administrator (usually, the security manager) does not delete them. The reports specify the audit results and remediation activities.

Requirement 12: Maintain a policy that addresses information security for all personnel.

12.3 Develop usage policies for critical technologies and define proper use of these technologies.

- Guidance: *„Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data. If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data."*[1]

- EPAS Coverage:

✓ EPAS Audit includes regularly updated password leaks obtained from known security incidents; this data is used by the password assessment process in order to determine if any of the accounts is using exposed credentials - such accounts are flagged immediately in order to start the remediation process.

✓ EPAS Enforcer is used to blacklist passwords which have already been exposed and are included in the leaked credentials database. Also, EPAS Enforcer provides granular and privacy compliant events whenever a password change occurs and whenever a password change fails due to password policy violations.

PCI DSS requirements supported by EPAS summary

PCI DSS Requirements	Description	EPAS Coverage
2.1	Change default passwords and remove unnecessary default accounts	✓
2.3	Encrypt non-console administrative access	✓
2.5	Security policy documentation and use	✓
2.6	Protect hosted environment and cardholder data	✓
5.4	Policy in place for protecting against malware	✓
6.1	Process to identify security vulnerabilities and assign a risk ranking to security vulnerabilities	✓
6.3	Develop applications securely	✓
6.7	Document security policies and operational procedures for developing and maintaining secure systems	✓
8.1	Proper user identification management	✓
8.2	Proper user authentication management	✓
8.4	Document and communicate authentication policies and procedures	✓
8.5	Do not use shared IDs	✓
8.8	Document security policies and operational procedures	✓
10.2	Implement automated audit trails	✓
10.5	Secure audit trails	✓
10.7	Retain audit trail history	✓
11.3	Implement a methodology for penetration testing	✓
12.3	Develop usage policies for critical technologies	✓

DETACK GmbH
Königsallee 43
71638 Ludwigsburg, Germany
Phone: +49 7141 69 62 65 0
Fax: +49 7141 69 62 65 5
info@detack.de
www.epas.de