epas

Enterprise Password Assessment Solution

Enriching User Authentication

epas

The process of Authentication

Passwords are still used across a wide range of corporate environments. Thus, security and risk management leaders in charge of IAM (Identity and Access Management) systems, must establish password policies in accordance with regulations and auditors' demands[1]. Still, legacy passwords are vulnerable to a wide range of attacks and, by themselves, are no longer suitable, except in minimal risk use cases. These regulations and demands can present little value in practice, while placing a burden on end users and security administrators alike. Therefore, IAM leaders can spend hours on designing the most appropriate corporate password policy, resulting in almost no improvements in security. A better approach would be to shift time and effort from password policies to more effective compensating controls. One solution that bolsters the single factor authentication and analytics-centric authentication methods (conditional authentication / MFA) can be found in EPAS (Enterprise Password Assessment Solution). It provides a legal, privacy-compliant password quality assurance process for all enterprise IT systems, offering also password audits and risk assessments. The solution is delivered through dedicated software and hardware infrastructure that connects to the customer's proprietary equipment, acting as an ADP (Authentication Decision Point), in addition to providing the necessary tools for securing existing credentials: audit, remediation, and compliance

The solution is delivered through dedicated software and hardware infrastructure that connects to the customer's proprietary equipment, acting as an ADP (Authentication Decision Point), in addition to providing the necessary tools for securing existing credentials: audit, remediation, and compliance.

Passwords Authentication and Weaknesses

Password policies cannot ameliorate the inherent weaknesses of passwords by themselves. Security and risk management leaders responsible for IAM should invest in other compensating controls in line with business needs[1].

The research "Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls" published by Gartner has successfully displayed all the limitations given by the use of weak passwords, driving the market to the use of alternative authentication methods. Due to the use of weak and predictable passwords, it is no longer retained appropriate to use them as an authentication method per se, but always coupled with another mechanism of authentication such as MFA (that results often in 2FA) or biometrics, introducing though some limitations.

Password policies are often not enough for assuring the use of valid passwords, they cannot evaluate, in most of the cases, the predictability from the mathematical or logical perspective; they can force, in the majority of the cases, the use of multiple group characters (alphanumerical, symbols, etc.).

Auditing a password is a difficult process to implement without landing in privacy violation, resulting in the disclosure of the clear text password. Nevertheless, enterprises must abide by such requirements. Policies must satisfy all compliance issues, from non-privileged to administrator users.

1 https://www.gartner.com/en/documents/3773163/don-t-waste-time-and-energy-tinkering-with-password-poli

This led to the use of a workable policy rather than a perfect one, pointing in improving the UX (User Experience). The introduction of "more robust authentication methods" has been unsatisfied so far. 2FA, biometrics, FIDO (Fast ID Online), tokens, etc. have solved some problems and introduced others, often resulting in higher complexity of the systems or insufficient compatibility. Within policies, it has been considered fundamental to avoid rules that drive counterproductive behaviours, for example demanding a long and complex password that usually results in bad behaviours like use of common patterns such as "Thisismypassword123" or even worse, in people writing down the password in unsafe places like post-it or phones. Therefore, a goal is to provide a satisfactory UX.

Thinking about reliable passwords, they are expected to possess a certain length and complexity level, meaning in a minimum of 8 characters (even though 10-12 is recommended) including different character groups (lower and uppercase, digits, symbols and so on). What usually is not taken into account, or is done in a very generic way, is the avoiding of common patterns or dictionary words (e.g. "password", "qwerty", "123456", "iloveyou"). It is also difficult to prohibit personal information such as name, surname, birthdays, pet name and so on. In the end, displaying the impossibility of the use of a non-conforming password without giving a reason leads to bad practice, because the user is not aware about what is considered a weak or predictable password. Thus, it has been evaluated as having a very positive impact, the use of a score for measuring the password strength of an end user. Password history is also a critical point, because most of the passwords are related to each other, meaning that a breach of an old password stored in weak hash, can be used by an attacker to guess the new one (maybe just an update from "myname2018" to "myname2019").

A threshold for a number of failed consecutive login attempts is suggested to avoid brute force attack on the login point, but should not affect the UX. Is recommended to use "penalty box" approaches, locking accounts only temporarily to avoid denial-of-service attacks and make the security team aware of a possible attack.
Avoiding password reuse is an important point complicated to accomplish. Password manager tools can, in part, fix this kind of problem, collecting all the passwords under an encrypted database with a long and complex master password. However, these tools may require considerable technical skills and are unlikely to save time and effort. Password aging has been considered inefficient, because it has been determined that the regular change of passwords does not significantly limit exposure to attack. A password change is recommended if a login happened in a shared public device or there are suspicions about the discovery of the password. Several controls that minimize the impact of an attack include monitoring and analytics tools (check concurrent logins from multiple unknown locations or outside of a normal working day), notification of last login, timely deprovisioning (disable accounts that are unused for a set period in the expected parameters) and using a CARTA (Continuously Adaptive Risk and Trust Assessment) approach.

Multi-factor authentication (MFA) and biometrics increase the effort required from an attacker to acquire the means by which to access an account, but all of this has a cost (not only given by additional hardware), and might impact the UX. Because of negative user feedback, major vendors have given up the requirement to use MFA for each authentication event, the trend is now to use as much as possible conditional authentication, with the password being usually the regular method, and with an additional factor when potential risks are detected. Apparently users did not like being forced to use multiple factors, recently this could be seen happening with the online banking in Germany, where permanent MFA was quickly dialled back to conditional authentication.

CARTA approaches are the trend now on the markets, meaning that use of passwords will be assured for the predictable future. Therefore, products and services that integrate rich analytics to enable a CARTA approach will be sought, specifically within enterprises that want to take a lean-forward stance to address advanced threats that exploit user credentials. The "continuous" element needs a special consideration. Tools that make a "risk-based" authentication decision at login provide less value than those which can make truly adaptive decisions throughout a session. In CARTA, access management tools are far better than pure authentication tools, however, across different use cases, conditional authentication will be sufficient in the near term. The most advantageous solutions include authentication methods that best provide the necessary balance among trust, TCO (Total Cost Ownership) and UX/CX (User Experience and Customer Experience) in each use case.

Although the prospect of a universal, high-trust authentication method may be attractive initially, it is usually overkill. Most users have access to only low- or medium-risk applications and data. High-trust authentication may be unnecessarily costly and impose too much friction.

About EPAS

EPAS is a patented (USPTO 9,292,681 B2, EP2767922) solution developed by Detack GmbH and its Swiss partner Praetors AG. Detack was formed in 2001 by a group of IT security consultants who set up a business focusing on IT security auditing and consulting in Germany and throughout Europe. Given the existing customer demand for solutions to address the use of weak or insecure passwords and lack of quality assurance in user authentication, EPAS was productively launched in 2013. As of 2019, EPAS was already deployed in over 30 countries, with several millions passwords being analysed on a weekly basis. The product is mature in terms of features, stability, developments and operations. 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, Linux/UNIX, IBM System z, SAP, database servers, and more. It uses a self-developed, patented technology in order to extract all relevant password data from a target system and to use this information as well as bundled intelligence data and analytics algorithms to assess the resilience of passwords against attacks. EPAS employs only legitimate cipher text extraction methods and therefore does not cause any system availability risk for the target. It has been designed to meet the needs of modern enterprises,with more than 30 different systems and databases, ranging from IBM, SAP, Linux/UNIX, Oracle to Microsoft, being supported. Legally compliant reporting offers all security relevant password data whilst respecting the protection of personal data and satisfying workers councils´ requirements. EPAS, an on-premises SaaS solution, is delivered through appliances which are integrated into the client's data center.

An optional licensed feature of EPAS is the Enforcer, which systematically prevents the use of weak, reused or shared passwords whenever the password is changed. It supports various systems, such as Microsoft A/D and local accounts, UNIX, web-enabled applications, etc. EPAS Enforcer for A/D integrates as an LSA (Local Security Authority) filter on the Windows Active Directory domain controllers and ensures that passwords meet defined security requirements when set or changed, in line with a centralized policy mandated by the risk category of the information they protect. The new password is tested against the EPAS evaluation criteria and is accepted or rejected, depending on the defined security requirements. This means that formerly permitted passwords like "Password123" or "Secret!" are not accepted any longer by the domain. If the password change attempt is unsuccessful, an optional feature of the EPAS Enforcer displays the failure reasons (e.g. "Password must not be included in a dictionary.") to the end user. The security requirements for a password result from the security classification of the data to be protected, based on customer specific measurements.

The EPAS appliance deployment architecture is tailored to each custom environment, taking into account parameters as the number of users, types of systems, number and location of data centres, and, especially for multinational enterprises, privacy and legal requirements. The unit that manages the logic behind the operations is the EPAS MASTER which facilitates the communication with the EPAS WORKERs and the EPAS AGENTs. These entities only handle the information and handle the business intelligence processes. The WORKERs contain GPUs (Graphics Processing Units) that are used for processing power. The EPAS AGENT is used to connect remote data centers or locations, to speed-up communications and ensure high availability and failover.

Market Presence of EPAS

EPAS is currently deployed within a wide range of industries such as BFSI (Banking, Financial Services and Insurance), metallurgical and chemical industries, resources (mining, energy) automotive, state and law enforcement, etc. EPAS has proven to be an excellent fit for various types of organisations, as reflected by the positive reviews given by some of its customers[2]. EPAS is the only legal, privacy compliant solution which can actually measure the resilience of existing passwords in more than just Windows environments, covering most of the known enterprise systems. Some competitors cover in a limited manner selected features present in EPAS, although no solution is known to offer the full set of capabilities; for example, the enforcement of strong passwords addressed upon dictionary based attack methods is also offered nu SPECOPS, Anixis, Microsoft Azure AD. EPAS enriches password management platforms and is often integrated with password reset platforms and PAM solutions, such as the one provided by CyberArk.

2 https://www.gartner.com/reviews/market/security-solutions-others/vendor/detack/product/epas

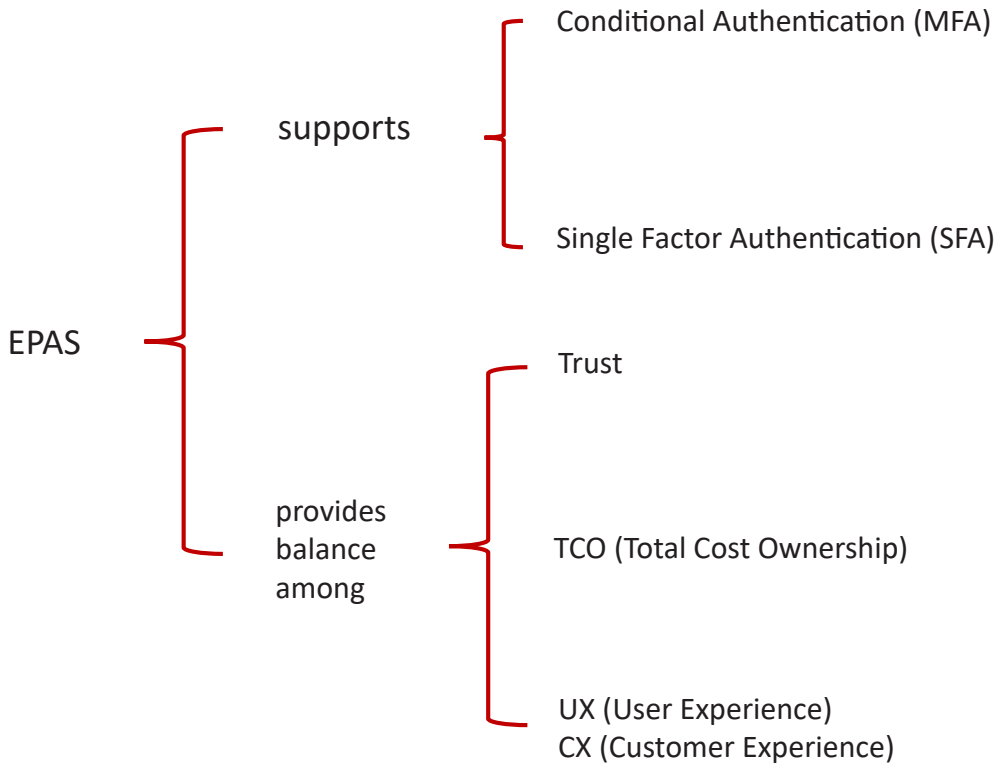
EPAS provides the baseline for the remediation of poor passwords, the definition of policies and measures both the progress and compliance. Identity Threat Intelligence provides ongoing quality assurance.

Often, organisations try to perform password audits and risk assessments using hacking or various public domain tools. This, however, violates privacy laws or local regulations recklessly in terms of security and requires a lot of effort. It also does not provide an objective assessment of the results: some passwords may be cracked, but there is no baseline available, no standard measurements and KPIs, and there is no objective way to classify a password as good or bad. Although the results provided by such methods might be interesting in respect to learning, they cannot be used for remediation, objective reporting, and compliance. This is how EPAS has evolved - customers wanted their passwords audited, but their workers councils would not allow standard approaches. Detack developed the ability to analyse passwords while preserving users' privacy, enforcing state-of-the-art password policies, and integrating in the password change workflow. Millions of users benefit today from this approach without suffering any privacy dilution.

How EPAS enriches the User Authentication process

User authentication refers to verification of a wide range of transfers of human to machine credentials which require the authenticity of the user for confirmation. The authentication services market is expected to grow from USD 507.0 Million in 2016 to USD 1,619.5 Million by 2022, at a Compound Annual Growth Rate (CAGR) of 21.1% during the forecast period[3]. Some of the key players operating in the user authentication market include Computer Sciences Corp. (Virginia, U.S.), CA Technologies Inc. (New York, U.S.), GermaltoNV (Amsterdam, The Netherland), SecureAuth (U.S.), VASCO Data Security International Inc. (Illinois, U.S.) and SecurEnvoy Ltd (U.K.) among others[4].

EPAS supports the use of the Conditional Authentication (MFA) and reliable Single Factor Authentication and it best provides the necessary balance among Trust, TCO (Total Cost Ownership) and UX/CX (User Experience/ Customer Experience) in each use case.



3 https://www.gartner.com/reviews/market/security-solutions-others/vendor/detack/product/epas
4 https://www.marketsandmarkets.com/Market-Reports/authentication-services-market-85067532.html

For assuring a high level of Trust, EPAS includes all the recent technologies in terms of ML (Machine Learning), resulting in an adaptive and custom analysis of every account. Looking at the historical passwords used during the lifetime of the user's account, EPAS is able to predict the behaviour of the user in choosing the new password as an attacker would do. In a very safe environment compliant with the user's privacy rights and expectations, EPAS will not allow a user to choose a password correlated to one that has been used before, even by another user. Password breaches, leaks, as well as any dictionaries disclosed on the Internet (both clear- and dark-web), are bundled (and constantly updated) with EPAS as dictionaries, preventing users to use passwords whose hashes are already known to malicious actors. This provides EPAS customers with up-to-date, expert knowledge in perfecting the user authentication environments.Password security is a dynamic, forever evolving metric which is affected by multiple factors. Some factors are technology-related (rate of recovery speed, usage of memory or CPU bound hashing function), while some factors remain bound to human parameters, such as: dictionary usage, leaked passwords, evolving patterns in choosing password, language or cultural patterns. EPAS evolves dynamically, constantly updates to take into account changes in all relevant factors.

The process of adopting a new User Authentication solution implies investments in technology, personnel training and it represents a critical point in terms of companies' costs. For reducing the TCO, EPAS is packed as a both hardware and software solution with no other complex dependencies required to be provided by the customer and is instantly usable to perform detection and remediation. The hardware provided is equipped with state-of-the-art technology in terms of computational power: EPAS is able to analyse billions of passwords within an average-sized environment in an acceptable time frame - an audit can finish in a few hours up to a few days; all the passwords recovered are measured, from multiple perspectives (password policy compliance, structural entropy evaluation, password recovery reason) and then discarded. Full-disk encryption, as well as verifiable hardware sealing mechanisms are implemented through the use of State-of-the-art TPM chips. The TPM key does checksum of all the hardware present in the environment, any modification at the given hardware will result in a failure-check and will keep the data within encrypted, thus impossible to retrieve. Also Physical measures are in-place to prevent theft (tilt, movement and chassis sensors).

Enriching UX/CX represents one of the primary goals of the solution. By implementing EPAS Enforcer, users will be more aware about the weaknesses of their passwords. Being given an explicit reason for which their passwords are being rejected, they can become more aware in using more strong and reliable passwords without impacting the UX. This has been demonstrated through the papers "Does my password go up to eleven? The impact of password meters on password selection", by S. Egelman and others[5], which found that strength meters motivated people to create stronger passwords. In "Password Creation: 3 Ways to Make It Easier", Katie Sherwin of Neilsen Norman Group says, "Visually representing the strength of the user's password, and showing that there is room for improvement, changes the motivation. The benefit is getting a secure password, instead of just complying with a system's arbitrary command. It's a slight mental shift that has a potentially large impact on security".[6] The score given by the Enforcer looks at the password from the mathematical, linguistic, and logical perspective, assuring that no dictionary word or common pattern has been used during the process of selecting a new password. Through the custom EPAS message, not only the use of a non predictable password is accomplished, enforcing trustiness inside the system, but also user education is provided without impacting UX.

5 https://dl.acm.org/doi/10.1145/2470654.2481329
6 https://www.nngroup.com/articles/password-creation/

EPAS fixes the problem of weak passwords with the Enforcer. Usually, most of the accounts are recovered by applying derivation rules to the known account information, doing simple transformations like using the number 4 instead of the A, the number 3 instead of an E, the "$" instead of the S, etc. Those are common transformations that allow compliance with most of the password policies and make the user itself feel safe against an attack, while he/she is actually not. An attacker knows about these transformations and will definitely try every combination in order to get access to the system. Also, hybrid rules to the known account information are applied, meaning appending and prepending characters. What is done with the known account information is repeated again with a provided dictionary. It is verified if the password has been recovered because it has been found in a dictionary (language dictionary like English, German, Arabic, etc. and other types of dictionaries such as recovered passwords dictionaries, publicly available ones, like the "rockyou" dictionary, or from some recent leakages like the Yahoo breach, LinkedIn breach, and so on).

To conclude, based on a patented technology, EPAS regularly analyses enterprise passwords, detecting anomalies, gathers threat intelligence and calculates a numeric, objective resilience of each password versus defined attack methods. This analytics is used to plan, implement and measure remediation programs, as well as the ongoing quality assurance of passwords. Attacks are simulated with real patterns and weak, shared, and Internet-leaked passwords are detected. EPAS can be used to perform scheduled or ad-hoc password audits and risk assessments across all enterprise environments. It is constantly used against thousands of productive systems on a regular, automatic basis, with zero impact on availability. Passwords are never stored, just measured, then discarded, so that remediation can be achieved without knowing the clear text. The assessment results in compliance reports, password quality KPIs, and detailed information for all management layers. The provided benefits include achieving strong passwords, preventing security incidents, and satisfying both internal and external compliance requirements.

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

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig