Synopsis

For 25 years, we have been conducting penetration testing, and we are still surprised by how many systems remain vulnerable due to insecure passwords. Despite multi-factor authentication being available for over 30 years, and passkeys or passwordless for over 20 years, weak passwords continue to be one of the leading causes of security breaches.

Ten years ago, we decided to take action. This led to the creation of EPAS, which is today the only solution capable of detecting and preventing insecure passwords without causing a privacy breach.

Currently, we protect several million accounts and some of the world's largest corporations. Since adopting EPAS, none of these accounts have been reported as compromised because of insecure passwords.

What is epas?

Challenge

It is an established fact that insecure, reused, and compromised **passwords** are one of the leading **causes of security breaches**.

A **password** alone is **not inherently an insecure method** of authentication. Like any other IT component, it requires **testing** and **quality assurance** to ensure it is secure.

The issue with passwords has been, until now, the lack of testing solutions, specifically to **simulate the actions** of an attacker attempting to crack them.

This was not due to a lack of password-cracking tools, but because **revealing the plaintext** password results in a **privacy breach**.

Solution

EPAS offers a unique approach by **identifying and preventing** insecure, reused, and compromised passwords **without breaching users' privacy**.

This enables organizations to effectively eliminate all password-related vulnerabilities while continuing to use a proven, well-known, and well-supported authentication method.

EPAS is **patented technology** used on thousands of servers and identity management systems by **several million enterprise users**, in over 30 countries. Since using EPAS, **none of these accounts have been reported as hacked because of insecure passwords**.

Implementation

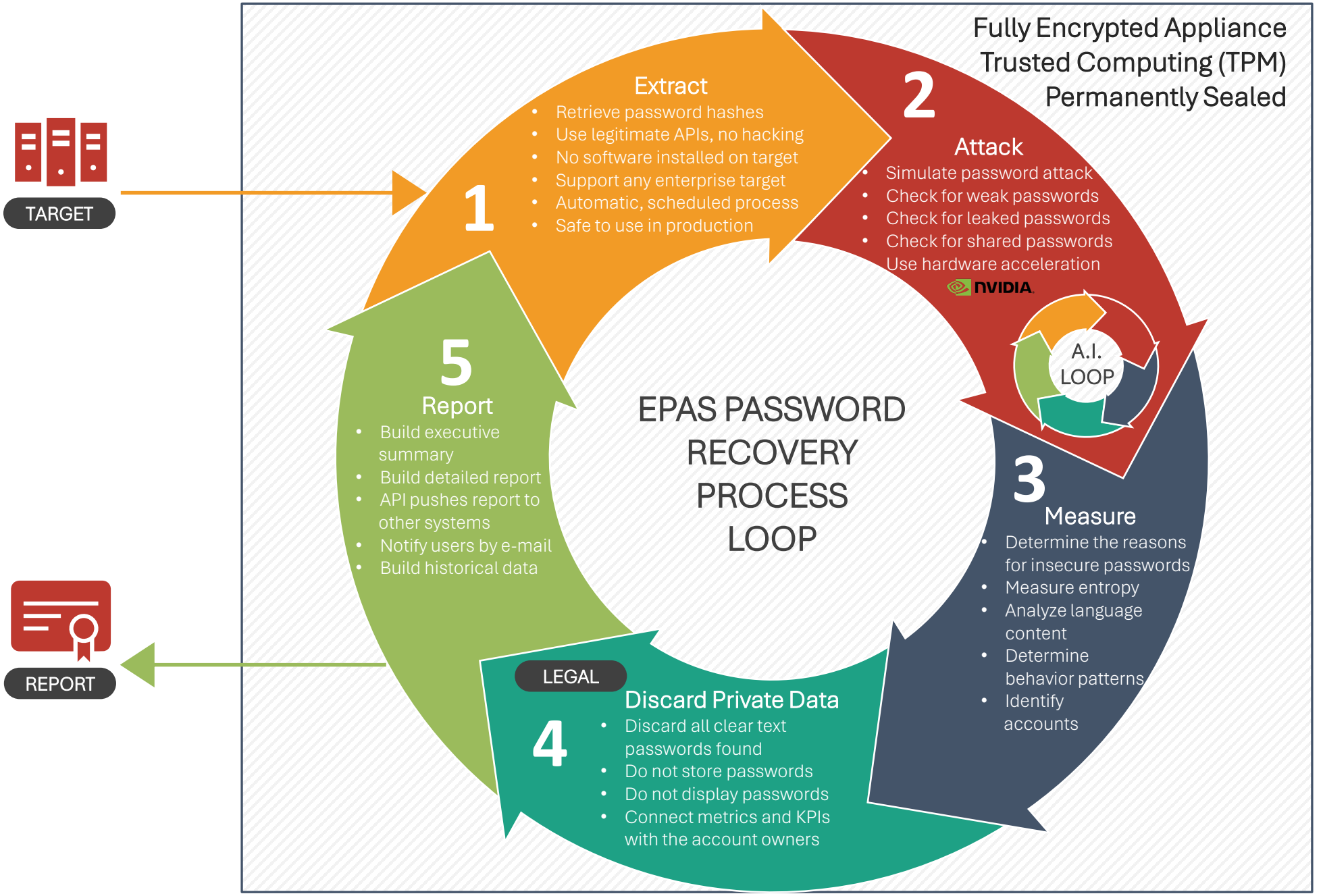
Using extra security measures like MFA and risk-based authentication is still **recommended to increase security**. However, this can often be challenging, especially for legacy and OT systems or when the necessary technology changes lead to very high costs.

The implementation can also take a long time, leaving accounts **open to password-related attacks**.

Even when MFA is used, the **password** is usually **one of the factors** and must be properly secured.

EPAS provides immediate protection, for **all passwords**, whether used as the only factor or **part of MFA**. The EPAS appliance is set up within **24 hours**, even in complex environments, and provides instant results, without installing any software on protected systems.

Patents: USPTO 9,292,681 B2, EP 2767922A1



EPAS represents the first solution to successfully address the challenge of conducting privacy-compliant password security assessments while simulating authentic attacks.

By executing the attack and evaluation within a sealed, secure environment, without storing or revealing the cleartext password, EPAS maintains full compliance with legal and privacy regulations. This pioneering development marks the first time a viable solution for implementing a comprehensive password quality assurance cycle has been made available.

epas

EPAS Specifications

Core Capabilities

- Detects weak, predictable, compromised, and reused passwords
- Simulates all known types of attacks, from brute-force to leaks and AI
- Does not expose or store the plaintext of recovered passwords
- Is applicable to both existing, encrypted passwords, and to new ones
- Prevents setting insecure passwords based on assessment metrics
- Supports all enterprise systems, from mainframes to Active Directory
- Protects both on-premises and cloud-based systems
- Bundles one of world's largest database of compromised credentials
- Leverages latest generation of GPU-based hardware acceleration
- Employs AI to identify passwords vulnerable to LLM-based attacks

Use Cases & Benefits

- Eliminate password-related security risks
- Meet regulatory requirements for authentication and privacy
- Optimize costs associated with identity management and authentication

Security Features

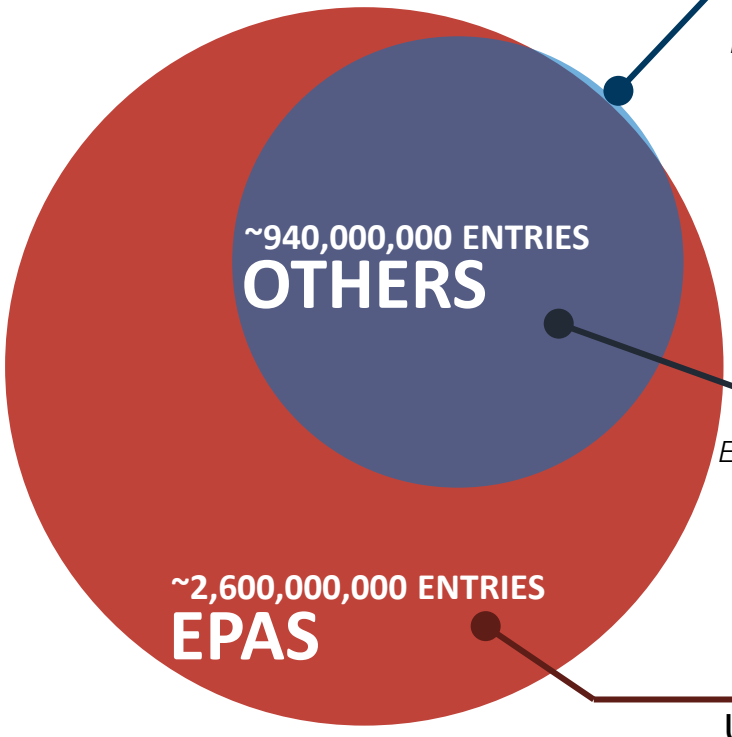
- Standalone hardware or virtual appliance, fully encrypted at all times
- Uses Trusted Computing with TPM for tamper prevention
- Fully isolated, with no external or Internet connection
- Production-safe, uses only legitimate vendors APIs for extraction
- Agent-less, does not install any software on audited systems
- Certified environment (ISO27001) and independently security tested

Integration & Enterprise Features

- Unlimited scalability across datacenters, countries, and cloud
- Provides full automation and scheduling without human intervention
- Provides APIs to integrate with SOC environments and 3rd party tooling
- Delivers enterprise grade reporting, metrics, and KPIs
- Readily available for MSP / MSSP use cases, with multi-tenant capability
- Regional support centers in USA, Germany, Singapore, Australia
- Mature, trusted technology used by some of world's largest corporations

EPAS Features: Compromised Credentials & AI Enhanced Password Audit

PASSWORD INTELLIGENCE SOURCES



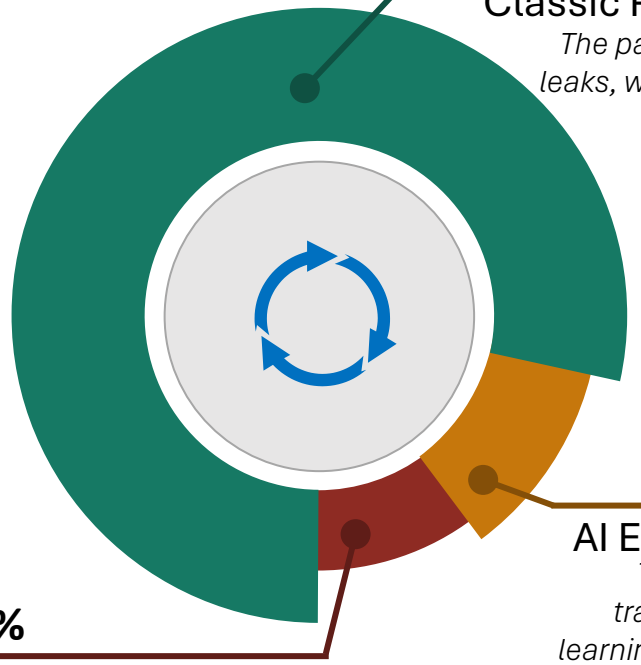
~0.1%
Not in EPAS
Entries found only in other sources

~36.2%
EPAS & Others
Entries found in EPAS and other sources

~63.7%
Unique to EPAS
Password entries only found in EPAS

Approx. 2.6bn unique plaintext passwords leaked between 2000-2024

AI ENHANCED CRACKING EXAMPLE



~75%
Classic Password Cracking
The password is found by using leaks, wordlists, brute-force, and derivation rules

~15%
AI Enhanced Cracking
The password is found by training and using machine learning on default and custom data sets (unique to EPAS)

~10%
Not Cracked
The password is not found

EPAS Features: Security by Design

FULLY ENCRYPTED

For all EPAS appliance types, data is permanently encrypted. Data at rest is also always encrypted. Full data encryption is mandatory for both hardware and virtual EPAS appliances.

TRUSTED COMPUTING

By securely sealing the encryption keys to a dedicated TPM, it is ensured that the EPAS functionality (including the privacy assurance) is unmodifiable, even by the system owner.

NO EXTERNAL ACCESS

The EPAS system is deployed entirely within the customer's on-premises infrastructure or private cloud environment. EPAS does not necessitate Internet access and is never accessed remotely by Detack personnel. All updates are downloaded and installed by the operator.

INDEPENDENTLY TESTED

The EPAS solution undergoes regular independent security assessments, executed as a white-box process by WithSecure (previously F-Secure), with the results being made accessible to all customers. Additionally, the Detack professional security testing team continuously monitors and evaluates the EPAS security.

CERTIFIED DEVELOPMENT

Detack is ISO/IEC 27001:2022 certified (42505-49-SI). The EPAS Enforcer plug-in is verified, certified, and digitally signed by Microsoft.

EPAS Testimonials – Used by World's Largest Companies

Gartner Peer Insights™

5.0 ★★★★★ May 5, 2020

Great solution for password analysis and quality enforcement

Reviewer Function: IT Security and Risk Management | Company Size: 30B + USD | Industry: Miscellaneous Industry

The functionality of EPAS is impressive. Integration and rollout were trouble-free, in spite of a very complex environment.

5.0 ★★★★★ Dec 3, 2019

"Implementation is easy and the ROI realized is almost instantaneous"

Reviewer Function: IT | Company Size: 3B - 10B USD | Industry: Finance (non-banking) Industry

The product is second to none but what sets the vendor apart is their personal support, service and knowledge. The Detack team as a whole provides best in class support and response to questions/issues.

5.0 ★★★★★ Nov 15, 2019

Constructive flexible vendor with stable solutions

Reviewer Function: Procurement | Company Size: 500M - 1B USD | Industry: Miscellaneous Industry

Constructive and pragmatic vendor with stable solutions at reasonable conditions. We've worked with them for six years in Europe, US, and Asia and the relationship is excellent. Feedback from the technicians is also positive. We will be happy to extend our agreement with them again. ...

5.0 ★★★★★ Dec 14, 2020

Detack EPAS - Exceptional product and service for delivering compliance for passwords

Reviewer Function: Project and Portfolio Management | Company Size: 500M - 1B USD | Industry: Insurance (except health) Industry

Detack are an excellent vendor to work with - providing exceptional support, deep knowledge and guidance on implementation. Various challenges occurred with logistics not due to Detack, but they resolved them with a great level of patience. The solution has been implemented and is ...

5.0 ★★★★★ Sep 30, 2019

Easy installation / maximum benefit for password-quality

Reviewer Function: General Management | Company Size: 50M - 250M USD | Industry: Finance (non-banking) Industry

First approved and certified solution for the automated quality analysis of passwords in the company, which can be installed and operated without any problems and which also complies with data protection regulations (no problems with works council & Co.). By using EPAS, we ...

5.0 ★★★★★ Oct 10, 2019

Implementation was very easy and fast, the support in case of troubleshooting is excellent

Reviewer Function: General Management | Company Size: 50M - 250M USD | Industry: Banking Industry

Very good and professional initial setup phase to implement the product in the infrastructure, Very good and professional support if any problems occur,

Selected EPAS References

French multinational insurance company, founded in 1816, worldwide presence.
Revenue: €100 billion EPAS users: 200,000

German specialty chemicals company, founded in 1873, one of the largest specialty chemicals companies in the world.
Revenue: €12.2 billion EPAS users: 35,000

International banking group headquartered in Milano, founded in 1998, world's 34th largest bank by assets.
Revenue: €20.3 billion EPAS users: 70,000

American financial services and insurance company that was founded in 1859.
Revenue: US$11.0 billion EPAS users: 17,000

Emirates Global Aluminium is a conglomerate with interests in bauxite and primary aluminium smelting.
Revenue: US$9.4 billion EPAS users: 8,000

Boursorama (BRS) is a French online financial group created in 1995 by Société Générale.
Revenue: US$1 billion EPAS users: 2,000

Germany's largest car insurance company, founded in 1933.
Revenue: €8.5 billion EPAS users: 17,000

Greek multinational financial services company, founded in 1916.
Revenue: €2.6 billion EPAS users: 10,000

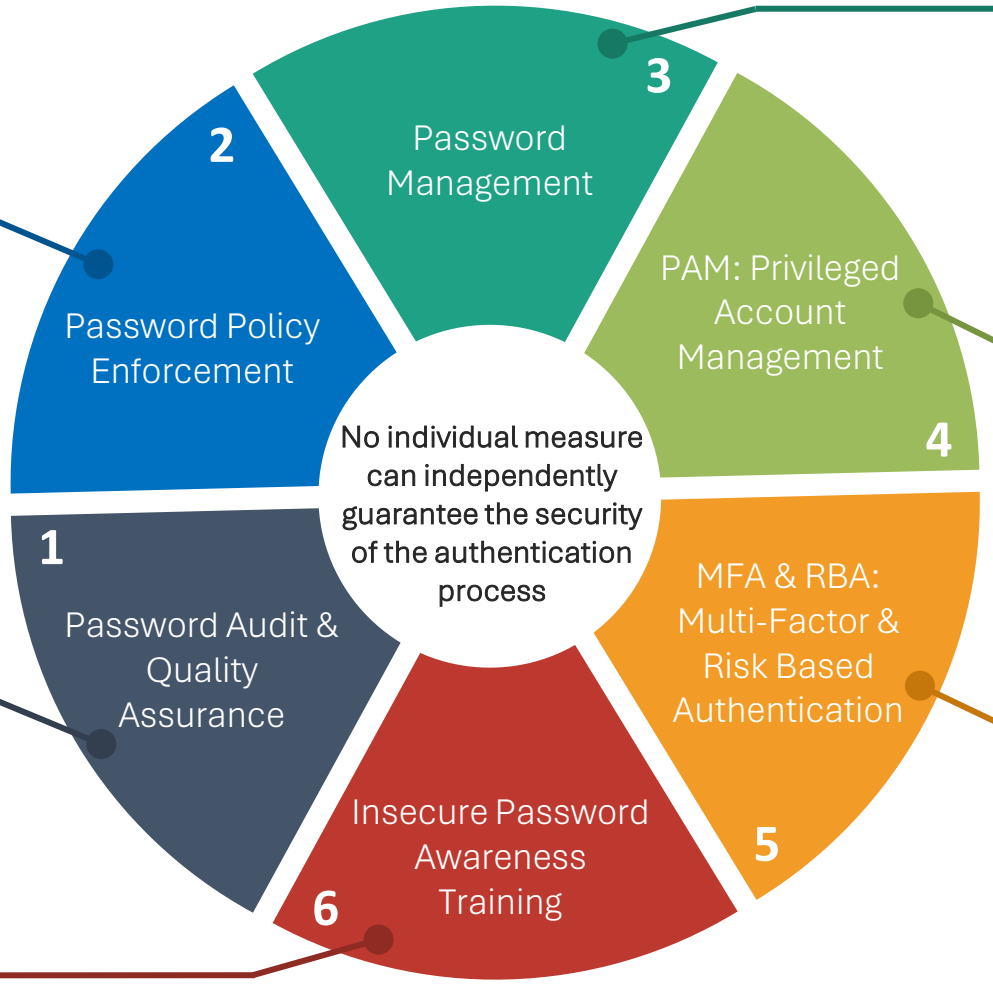
Atruvia provides IT services for 169,000 banking workstations and ATMs, administers roughly 82 million banking accounts, and serves 900+ banks.
Revenue: €2 billion EPAS users: 10,000

American insurance company founded in 1986, operating internationally.
Revenue: US$10 billion EPAS users: 10,000

More information available at: https://www.epas.de, https://www.detack.com, https://www.gartner.com/reviews/market/security-solutions-others/vendor/detack/product/epas

Differentiators vs. Other Password Security Technologies

Complementary Measures for Password Authentication Security



Block the usage of weak, compromised, or shared passwords at the time of password change.

EPAS & OTHERS

Identify if any of the passwords currently in use are weak, compromised, or reused, and act accordingly

EPAS ONLY

Train users to use secure passwords and to avoid password reuse

EPAS & OTHERS

OTHERS

Secure storage of credentials, simplified password entry, enterprise single sign-on

OTHERS

Automatic password rotation and policy enforcement for privileged users

OTHERS

Extended factors for additional authentication for critical access (VPN) or for challenging suspicious activity

Various measures and corresponding technologies exist to guarantee a secure authentication process. However, relying on a single technology is insufficient. Instead, a robust and reliable authentication security can only be achieved by effectively utilizing a combination of measures in tandem. Crucially, the ability to audit passwords in a privacy-compliant manner is exclusively provided by the EPAS solution.