WHITE PAPER

Device-Bound Access Security

Peig

Cloud is Taking over while Security Fails to Keep up

Cloud productivity services focus on being best at one thing rather than being mediocre at everything – a winning business strategy. Organizations take advantage of several specialized single-purpose services that solve individual business problems exceptionally well. As a side-effect, **managing access security in a fragmented service environment is proving difficult.** To make things worse, with a growing dependency on cloud services cyber threats are rising steadily. Leading the way in successful cyberattacks, hackers take advantage of human error and credential theft to profit from accessing sensitive data.

In battling credential theft, state-of-the-art access management solutions have grown beyond coherence. **The industry has evolved around a plethora of technical solutions, where each one is a remedy for another:** *Where passwords are not enough, use Multi-Factor Authentication! When MFA hinges productivity, use SSO! When SSO becomes too risky, add adaptive authentication!*

A patchwork approach to access security is no longer sustainable. With an increasing demand for BYOD and cloud services, cyber threats have become a mainstream existential risk for businesses, with common cyberattacks often resulting in severe financial losses, deterioration of customer trust, or even bankruptcy. Addressing access security requires a comprehensive solution that resolves fundamental access vulnerabilities at their root.

Peig introduces a device-bound access security model that closes the access security gap and mitigates most prominent cyber threats by design. In doing so, organizations increase their access security confidence on all user devices and on any network. Human-centred by design, Peig ensures end users never struggle with authentication fatigue and organizations face no downtime while keeping access security under control.

Identity & Access Security Legacy

Access security and BYOD

Managing access security responsibly in a BYOD environment, where personal devices interact with company systems, presents unique challenges. As companies adopt more SaaS tools and accommodate increasingly more diverse workforces and BYOD policies, the complexity of managing security has significantly increased. The issue is exacerbated by the wide array of siloed applications, each with proprietary user management systems and varying access security designs.

The lack of a unified access security approach in BYOD setups makes managing systems securely a substantial challenge for both security and IT teams. As remote work continues to rise, achieving security objectives typically adds layers of user friction, security complexities and operational overhead.

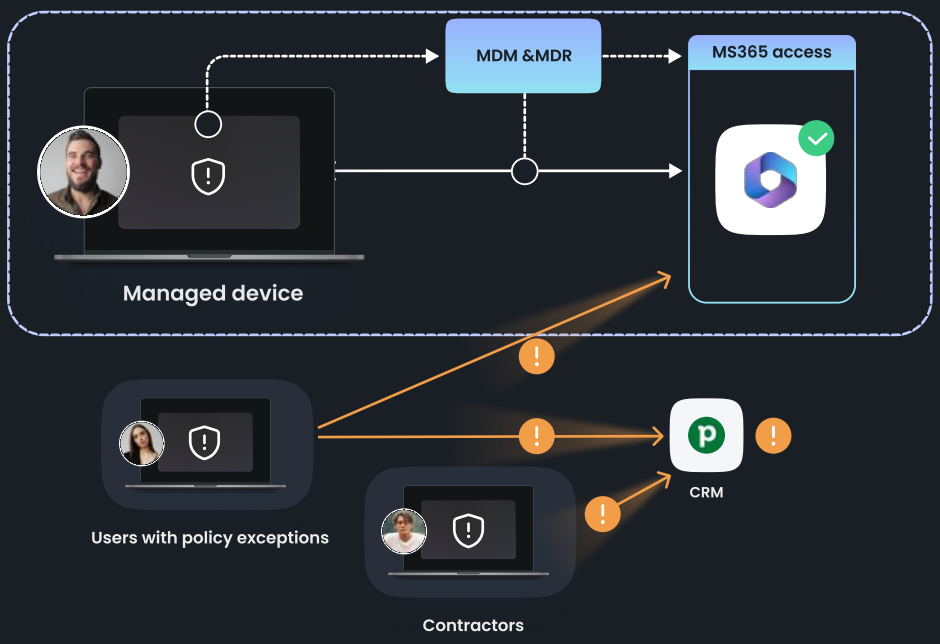
To address these challenges, businesses must adopt holistic access security solutions designed to also accommodate BYOD while safeguarding sensitive data and maintaining operational efficiency.

Use of stolen credentials

Credentials remain a significant weak point in enterprise security. Stolen or compromised credentials are a leading cause of breaches, with attackers exploiting weak or reused passwords to gain unauthorized access. The growing complexity of managing credentials across users, devices, and applications only amplifies the problem.

While stronger authentication methods like MFA are often suggested, they are far from a perfect solution. MFA implementations can introduce friction for users, leading to workarounds that weaken security, and fail to address the underlying issue: passwords themselves are inherently flawed.

To address this critical security gap, enterprises need innovative, device-bound passwordless approaches that eliminate the risks associated with credentials altogether, offering stronger security while simplifying access for users.



Traditional access security model

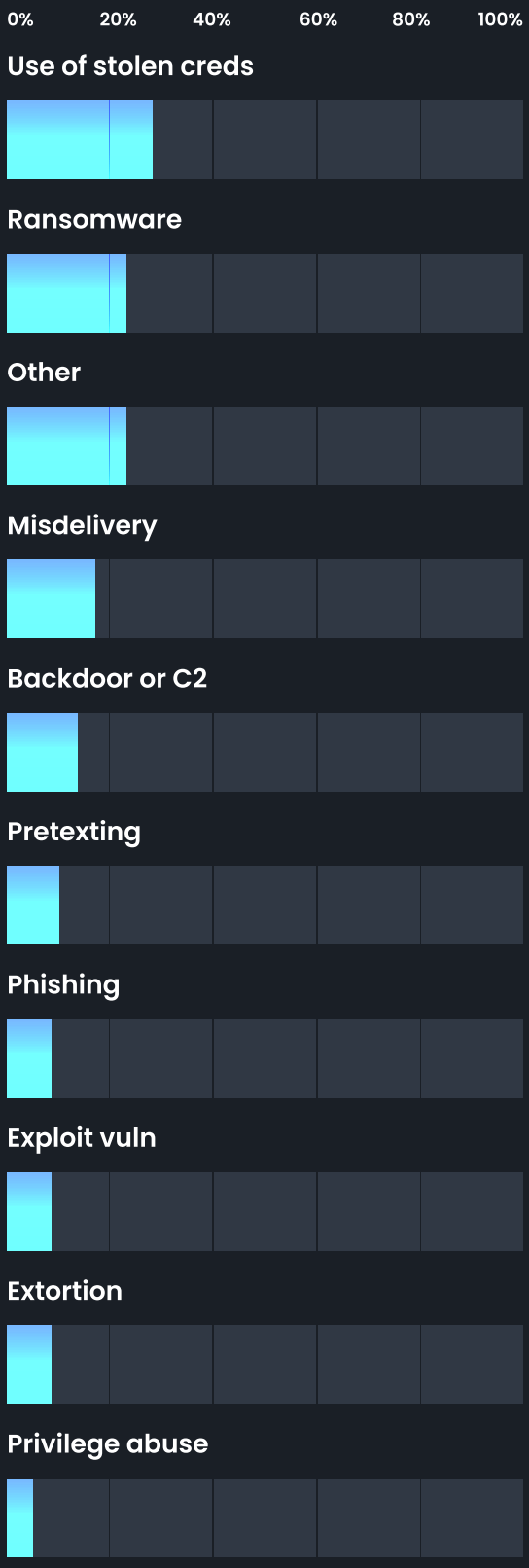
Rising cyber threats

According to Verizon's 2024 Data Breach Investigations Report,[2] **use of stolen credentials was the top action in breaches, accounting for 24%,** closely followed by ransomware at 23%.

According to Enterprise Management Associates[3] (EMA) **nearly 80% of TLS certificates on the Internet are vulnerable to Man in the Middle (MitM) attacks**, while as many as 25% of all certificates are expired at any given time.

As cyber threats continue to rise, the need for robust, device-bound access security has become vital. **Organizations must adopt more robust access security measures, including session-bound and resource-specific access verification tied directly to authorized devices.**

This approach not only strengthens defense capability against current threats but also reduces reliance on disruptive authentication workflows. Traditional MFA often imposes hidden costs on productivity and contributes to employee frustration. **Device-bound access security** mitigates these issues by enabling **seamless verification that aligns security with usability, ensuring that access is both secure and efficient.**



DBIR 2024: Top action varieties in breaches (n=9,982)

Access security is entangled

Trapped in legacy, access management vendors offer portfolios of double-edged solutions. Single Sign-On, Multi-Factor Authentication, adaptive MFA, notification-based passwordless or passkeys that may freely be copied between devices are some common methods that attempt to improve access security. Each fall short to address common business & security needs.

Single Sign-On (SSO)

⊕ Increases user convenience by providing a single set of credentials.
⊕ Increases usability with session cookies that don't require repeated authentication.
⊖ Increases risk by centralizing access security in a single point of failure.
⊖ Significantly reduces security confidence: session cookies = common point of exploit.

Multi-Factor Authentication (MFA)

⊕ Increases security because real users are required to confirm authentication with an additional device-bound factor.
⊖ Reduced user experience since users must take additional steps.
⊖ Dependency on an additional device.
⊖ Hard recovery in the case of loss.

Adaptive MFA

⊕ Reduces the number of times MFA is required.
⊖ Based on behavior analytics - attackers learn to forge behavior.
⊖ In critical situations, adaptive MFA further undermines the effort to recover.

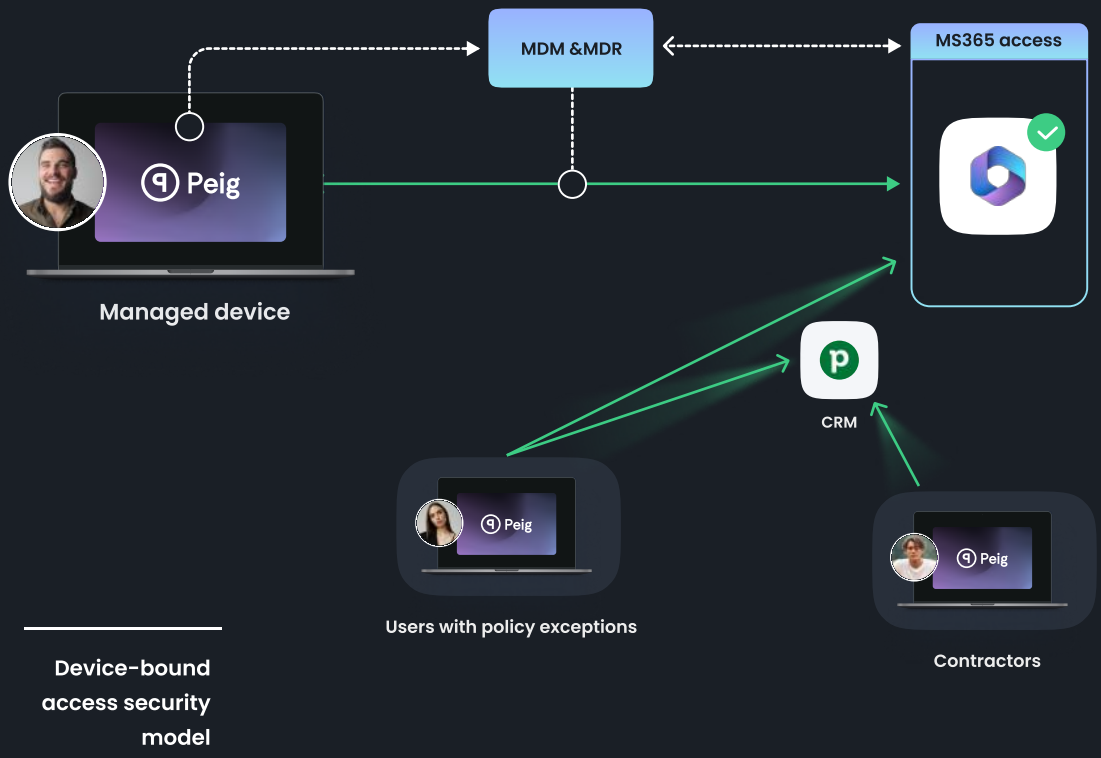
Passkeys

⊕ No need for passwords, which are hard to remember and manage.
⊖ Doesn't address modern MFA-bypass, phishing & MitM vulnerabilities or session takeover.
⊖ Violates cryptography management principles.
⊖ Not device-bound & our-of-scope for security teams.

Building security improvements of a legacy approach to access security proves to diminish reliability and utility. The username & password as a foundation for secure access results in layers of technical compromise.

Device-Bound Access Security

Device-bound access security is a method of securing access to systems or data by linking authentication directly to specific admin-authorized devices. This approach ensures that **only authorized devices equipped with Peig can establish a connection to sensitive resources.** By doing so, it adds a robust layer of protection, significantly reducing the risk of the use of stolen credentials, MFA bypass, session hijacking or cookie theft.



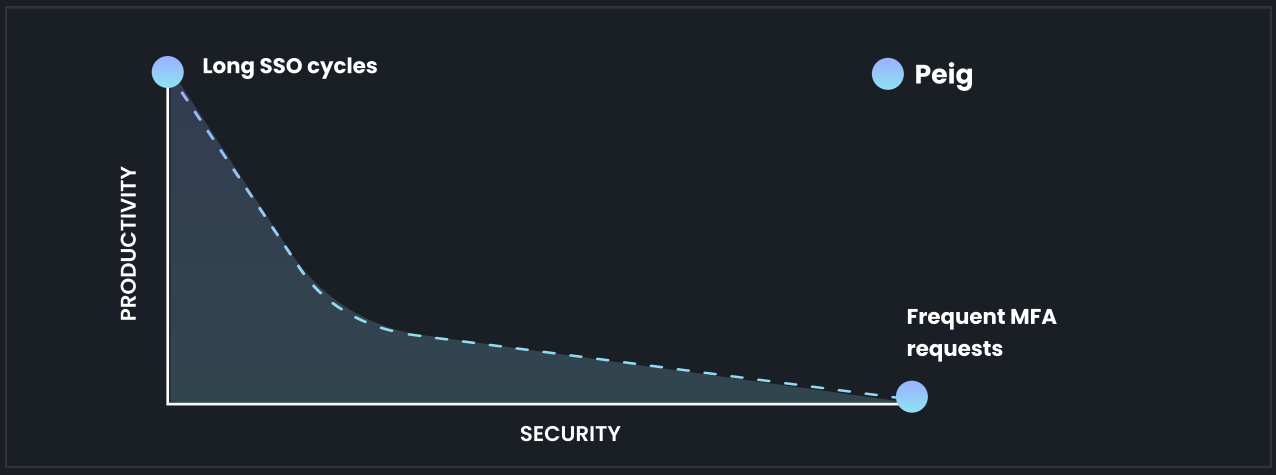
Device-bound access security model

Peig replaces the password with a device-bound and cryptography-based access security design. In doing so, Peig manages to:

- **Undermine critical vulnerabilities** including spear phishing, MFA phishing, MitM, session hijacking, cookie theft, as well as traditional password vulnerabilities like dictionary, or brute-force attacks.
- **Eliminate the need for additional HW tokens** or dependency on smartphone authenticators when working on desktop, or in BYOD friendly teams.
- **Reduce time spent on user authentication** and reduce **effects of authentication fatigue**.
- **Diminish downtime** in user or device **onboarding** .
- **Eliminate adaptive authentication downtime** in WFH, travel or after-hours work situations.
- **Simplify access** and security policy barriers to a minimum.
- Deliver **integration flexibility** to eliminate adoption barriers.
- **Enforce reliable Zero Trust** for private/public cloud or on-prem systems.

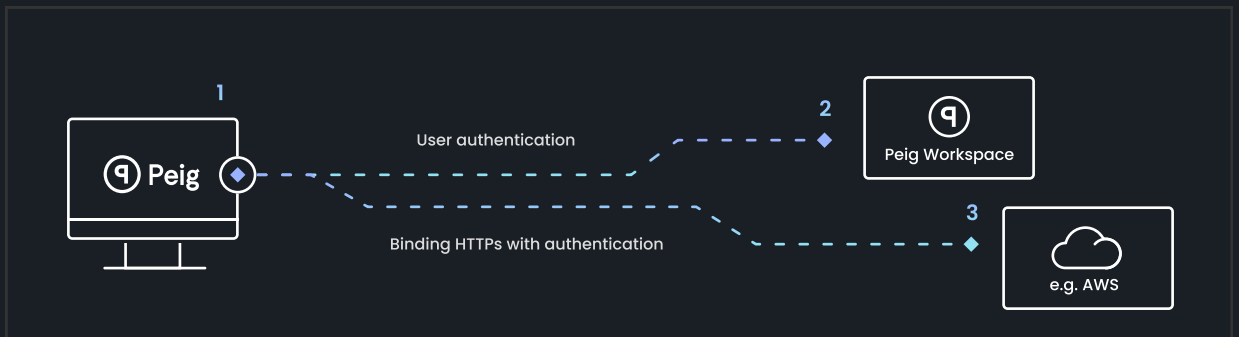
Untangling access compromise

Peig eliminates the need to balance security and convenience. Access security is no longer a question of intricate and case-specific risk assessment. Device-bound and secure-by-design Peig always maximizes both usability and cybersecurity. Contrary to traditional access security designs, Peig always maximizes the number of meaningful device-bound authentication instances so that **more authentications = more security = better user experience**.



The Peig device-bound architecture is built on automated identifiers and cryptography management. Users are not exposed to credential usage and management. As a result, employees are not required to undergo security training and practice a strict security policy that leaves room for human error. Peig challenges the status-quo, where security policy often expects unrealistic behavior, including periodically changing and remembering long passwords or spotting MFA spear-phishing emails. Peig security measures instead rely on advanced cryptography management and reliable automated authentication algorithms under the roof.

The vast majority of access-related cybercrime results from underperforming access security online**. Login credentials and MFA must be replaced by much stronger and more dynamic counterparts**. Taking full advantage of our devices' computing power, Peig is based on reliable cryptography, mutual authentication, TLS session binding and end-point cryptography security.



1

Authentication credentials

- Users don't need credentials or MFA to login
- Peig self manages and dynamically secures authentication cryptopgraphy

2

Mutual Authenticaiton

- Peig App & Service mutually authenticate to ensure user, device and network security

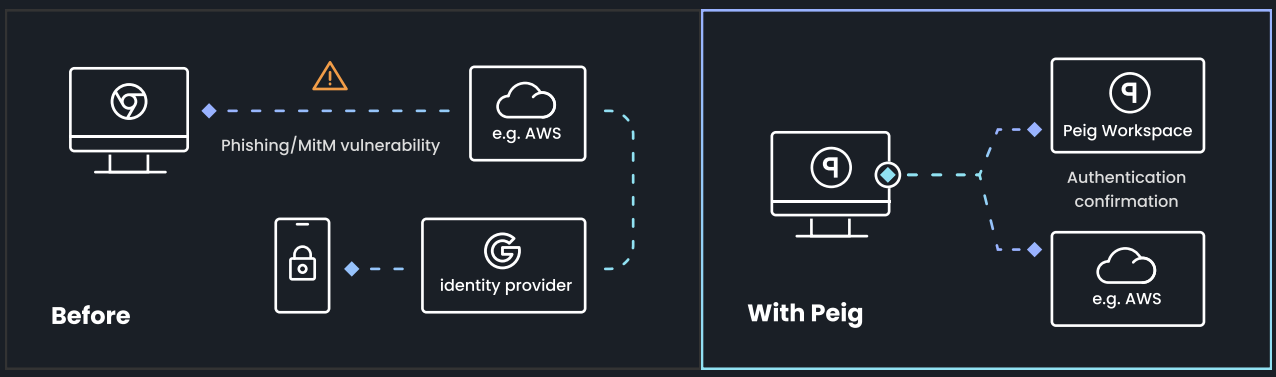
3

TLS key binding

Authenticating target application TLS session keys eliminates phishing & MitM

Fixing green certificate HTTPS security

Fixing access security requires fully closing the gap between session channels and authentication. Up to today, authentication security rarely had anything to do with session security. MFA apps authenticate users in a separate channel and hope for the best. This insufficient approach is an open door to phishing & MitM attacks. Peig closes the gap by using the full potential of HTTPS. **The architecture combines Peig cryptography to authenticate TLS keys used in HTTPS. In doing this, Peig re-established trust in "green certificates" and standard TLS encryption.**



Peig: A workspace browser as an end-point

Peig, a dedicated device-bound workspace browser, enables users to access resources securely. **Each browser instance is device-bound and authenticated with each access request**, allowing sessions with web services only for verified Peig instances and their rightful users.

Dynamic access security on end-point

HW-based key protection is no longer plausible for access protection. HW tokens are difficult to distribute and manage over time resulting in undesirable downtime in case of loss or malfunction. On the other hand, cryptographic data used for access security needs to be well protected. **To ensure access key security, Peig uses layers of periodical mutual verifications to ensure the cryptography hasn't been tampered with and to offer additional malware protection.** In case security keys are moved or misused, Peig detects an end-point attack attempt.

Cookies security reinforced

Peig temporarily stores web session cookies in RAM, reducing exposure to on-device malware. This approach greatly minimizes the risk of attackers stealing and reusing session cookies from other devices to gain unauthorized access. At the same time, it ensures a seamless user experience while supporting organizations in adopting Zero Trust "always verify" principles.

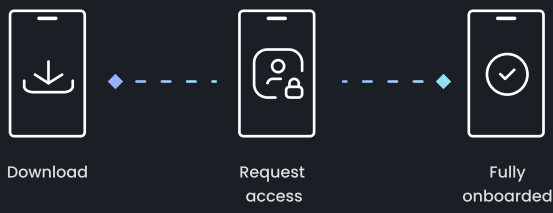
Productivity & user experience

Peig design minimizes user verification interaction to invisible. Users no longer need to type passwords, pull out their phone for authentication requests or use HW tokens to work in a top security environment. Users access company services directly from Peig just like they would from any browser because Peig is built on Google's Chromium browser to make the experience completely familiar while adding unprecedented levels of security that end users don't need to worry about.

- Save time authenticating
- Eliminate authentication fatigue
- Reduce employee stress

Device-based onboarding

To eliminate downtime and lengthy onboarding processes, employees may onboard their device remotely without technical support or HR help. Training non-technical admins authorize an onboarding request for users on managed devices, as well as BYOD. Authorized employees gain access to enterprise resources based on their access rights and only from an authorized device. From this point, repeated device-bound user authentication is invisible to the end user but always happens under the hood of every Peig application.



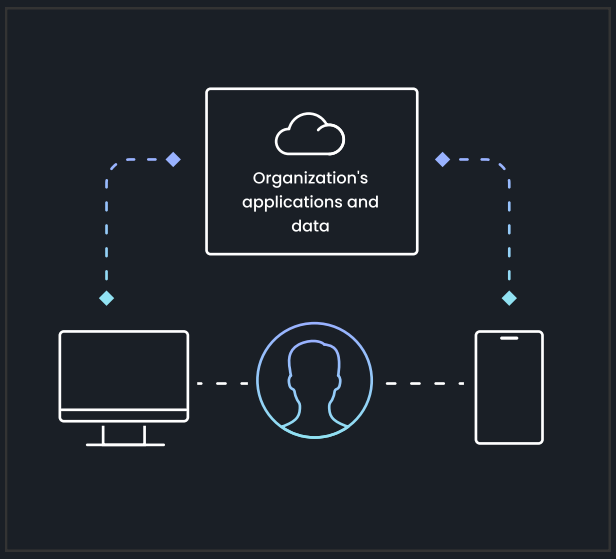
- Onboard new teammates instantly
- Reduce/eliminate downtime due to device loss, etc.
- Work fully remote

One device & any device

Working remote is possible on all employee's devices. **Users always only use the one device that is right for the task at hand to access their organization's resources.**

Employees may also onboard additional devices on their own to access company resources securely. In doing so, a desktop not only becomes an access point, but also a backup for an employee's smartphone in case of loss or malfunction.

While it's easy for users to onboard new devices, admins always have the last say. Admins are always in control of device access policy, letting them choose what devices a particular user can/cannot use to access company resources.

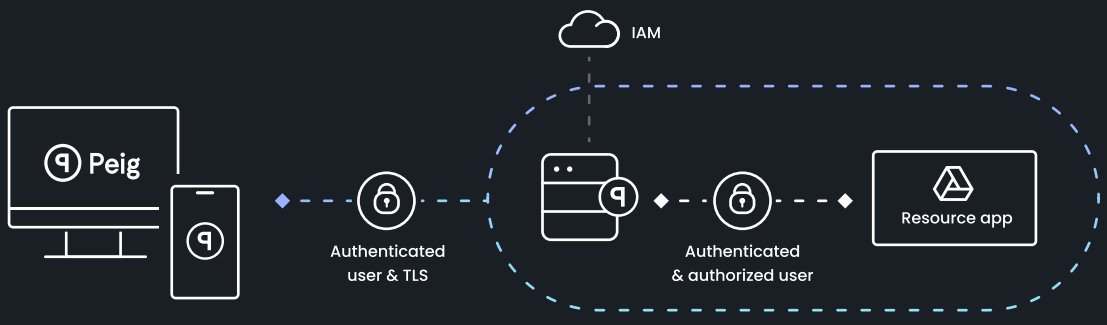


Workspace in Zero Trust

Once onboarded, employees can immediately access only applications and resources in the workspace for which they have been authorized. Leaving perimeter security behind, resources are independently protected, respecting Zero Trust security methodology.

Private-cloud and on-premises resources may each have an independent policy enforcement point (PEP), which are all centrally managed.

Access rights are consistently immediately enforced to maximize control over who can access what at what time. In doing so, employees access the minimum number of sensitive resources and for minimal time periods. Unauthorized access security risks are minimized as a result.



Private cloud & on-premise workspace in Zero Trust

Offering a whole new concept of enterprise data security, **Peig provides unique device-bound access security for all businesses.** Like a finely tuned race car, Peig is built for peak performance with all required security hidden away with no compromises made. Each second not spent navigating outdated security procedures is a second spent building up your company. **Built for SaaS, private cloud, hybrid, or BYOD friendly organizations, Peig is designed to be easily integrated and utilized with any number of business applications.**

SOURCES

1) "Cloud Computing Market Size, Share, and Trends 2025 - 2034" accessed January 29, 2025, https://www.precedenceresearch.com/cloud-computing-market

2) "2024 Data Breach Investigations Report | Verizon," accessed January 29, 2025, https://www.verizon.com/business/resources/T1f/reports/2024-dbir-data-breach-investigations-report.pdf

3) "EMA Report Finds nearly 80% of SSL/TLS Certificates are Vulnerable to Man in the Middle Attacks", accessed January 29, 2025, https://www.businesswire.com/news/home/20230801017674/en/EMA-Report-Finds-nearly-80-of-SSLTLS-Certificates-are-Vulnerable-to-Man-in-the-Middle-Attacks