e-guide

Access Management
Choosing Control over Cloud

The case for on-premise access management solutions

SecurEnvoy
A Shearwater Group plc Company

Executive Summary

In an era dominated by cloud-first strategies, the need for retaining absolute control over data and systems remains paramount for many organisations.

This e-guide provides a comprehensive overview of access management solutions and delves into the benefits of using on-premise access management to meet the unique needs organisations have for enhanced security, meeting regulatory compliance, and achieving cost-effectiveness.

We will also take an introductory look at SecurEnvoy's versatile approach to bolstering access management security.

Read on to find out more about how on-premise access management can help your organisation.

Contents

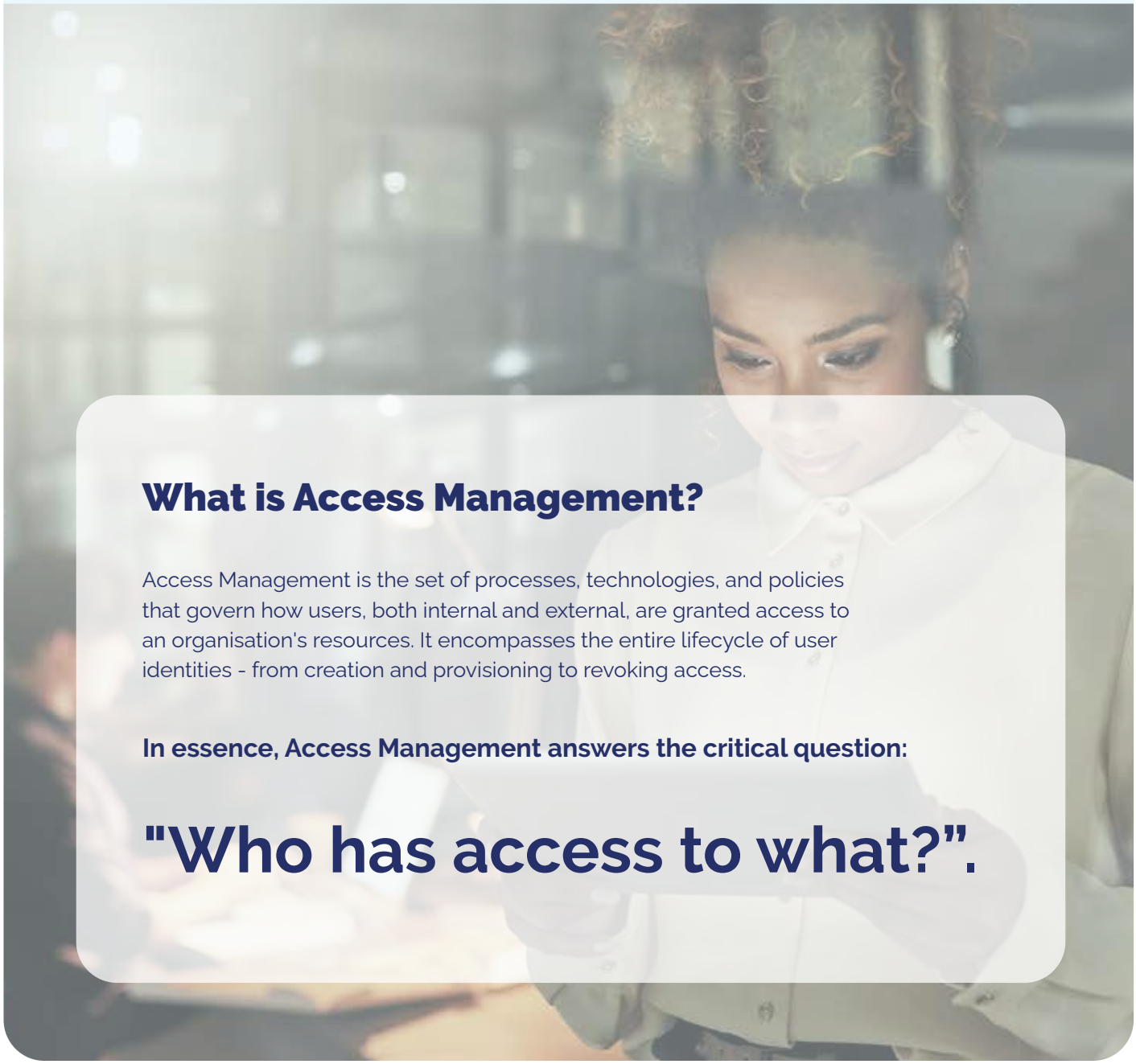
On-Premise

The need for Access Management

In today's hyper-connected digital landscape, where the exchange of information happens at lightning speed and data reigns supreme, the concept of Access Management has evolved from being a mere administrative function to a fundamental pillar of organisational cybersecurity.

Access Management, often referred to as" Identity and Access Management" (IAM), is the linchpin that controls who can access what within an organisation's digital ecosystem. It serves as the gatekeeper, ensuring that only authorised individuals gain entry to systems, applications, and sensitive data.

As we delve into the complexities of Access Management, it becomes clear that its significance extends far beyond mere convenience.



What is Access Management?

Access Management is the set of processes, technologies, and policies that govern how users, both internal and external, are granted access to an organisation's resources. It encompasses the entire lifecycle of user identities - from creation and provisioning to revoking access.

In essence, Access Management answers the critical question:

"Who has access to what?".

The Role of Access Management in Modern Organisations

Access Management plays a pivotal role in the digital age, where the security and privacy of sensitive information are paramount. Its significance can be summarised in two key aspects:

Security

Access Management is the first line of defence against unauthorised access and potential data breaches. By controlling who can access specific resources, organisations can protect their digital assets from cyber threats, both internal and external.

Robust authentication mechanisms and access controls are essential components of a comprehensive security strategy.

Compliance

In an era of stringent regulatory requirements, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS), compliance is non-negotiable.

Access Management ensures that organisations adhere to these regulations by accurately managing user access and conducting thorough auditing and reporting.

10 reasons why SaaS Access Management Deployments may not be an Option

There are several different situations in which organisations may choose or be required to avoid Public SaaS/Cloud deployments of an access management solution and opt for on-premise deployments. Here are some common scenarios where on-premise deployment becomes a preferred or necessary choice:

1) Stringent Data Residency and Sovereignty Regulations

Certain industries, like healthcare, finance, and government, are subject to strict data residency and sovereignty regulations. These regulations require that sensitive data remains within specific geographic boundaries or under the direct control of the organisation. Public cloud deployments might not guarantee compliance with these requirements, making on-premise solutions the preferred option.

2) Highly Sensitive Data Handling

Dealing with extremely sensitive data, such as classified government information or proprietary intellectual property, often means that organisations need to maintain direct control over their data. On-premise solutions can offer a higher level of security and control compared to public cloud options, reducing the risk of data exposure.

3) Customisation and fine-tuning

Organisations with unique access management needs or complex infrastructures may find it challenging to adapt public cloud solutions to their specific requirements. On-premise deployments allow for more extensive customisation and fine-tuning of access policies and authentication methods.

4) Legacy Systems Integration

Legacy systems that are not easily migrated to the cloud may require an organisation to opt for on-premise access management solutions. In such cases, integrating on-premise solutions with existing infrastructure can be more seamless.

5) Security and Control Priorities

For organisations that prioritise control and security, on-premise solutions enable security protocols, network configurations, and encryption methods to be established, maintained, and tailored to their precise needs, reducing the risk of security breaches.

10 reasons why SaaS Access Management Deployments may not be an Option (Contd.)

6) Concerns about Third-Party Access

Some organisations are wary of granting third-party cloud providers access to their critical systems and data. On-premise solutions eliminate this concern as all management and control reside within the organisation's boundaries.

7) Limited Internet Connectivity

In regions or industries where internet connectivity is unreliable or limited, relying on a public cloud-based access management solution may lead to operational disruptions. On-premise deployments operate independently of external network connectivity, ensuring consistent access control.

8) Cost Considerations over the Long Term

While public cloud solutions often have lower initial costs, they may become costlier over the long term as usage scales. Organisations with predictable and stable workloads may find that the total cost of ownership for on-premise solutions, including hardware and maintenance, is more cost-effective in the long run.

9) Organisational Policies and Culture

Some organisations have established policies or a corporate culture that favours on-premise solutions. They may have historical experience and expertise in managing on-premise infrastructure, making it a more comfortable and familiar choice.

10) Risk Mitigation Strategies

Organisations that have experienced data breaches or security incidents in the past may opt for on-premise solutions as part of their risk mitigation strategy. They can exercise greater control over security measures and reduce reliance on external providers.

Introducing SecurEnvoy Access Management

With an established track record spanning over two decades and a global clientele covering 36 countries, SecurEnvoy has a profound understanding of the multifaceted nature of business requirements and acknowledges that the concept of a universal solution is increasingly inadequate.

The demand for Software as a Service (SaaS) solutions, is undeniably driven by their ease of use and scalability for all industry sectors, and there has been a surge in demand from Small and Medium-sized Enterprises (SMEs). SMEs, however, are often constrained by limited internal resources and expertise and need the support of Managed Security Services Providers (MSSPs) to navigate the intricate realm of access management.

In addition, a trend is emerging for organisations to require direct control over the deployment of access management solutions. This requirement is fuelled by a commitment to data sovereignty and the preservation of supervisory authority. Recognising this paradigm shift, SecurEnvoy is able to accommodate diverse preferences with a spectrum of flexible deployment alternatives.

SecurEnvoy offers a wide range of deployment options, whether your organisation is looking for the convenience and worldwide accessibility provided by a SaaS solution, the assurance of a fully managed service available through our extensive MSSP partner network, or the flexibility to deploy a software image within your own physical data centre or private cloud tenancy.

Deploying SecurEnvoy Access Management

The SecurEnvoy Access Management solution offers a swift deployment option, allowing for a comprehensive on-premise implementation.

SecurEnvoy provides a Docker Compose script that will automatically deploy and configure the necessary components to run the solution on your own infrastructure.

Our Docker images require a Linux operating system to run on, but can be run inside Windows via Windows Subsystem for Linux (WSL) or your virtual machine platform of choice.

The Capabilities of SecurEnvoy On-Premise Access Management

Merging User Identities

Owing to mergers, acquisitions, and system migrations, organisations often find themselves in a situation where users possess multiple digital identities. At the heart of the SecurEnvoy Access Management solution lies the universal directory, a key component that enables the consolidation of these disparate digital identities into a single, universal user identity. This merging of user identities not only enhances security but also elevates the overall user experience.

Passwordless Authentication (FIDO2)

For a frictionless user experience, Passwordless Authentication leveraging FIDO2 passkeys can be enabled, removing the burden of the password from the user, increasing both convenience and security.

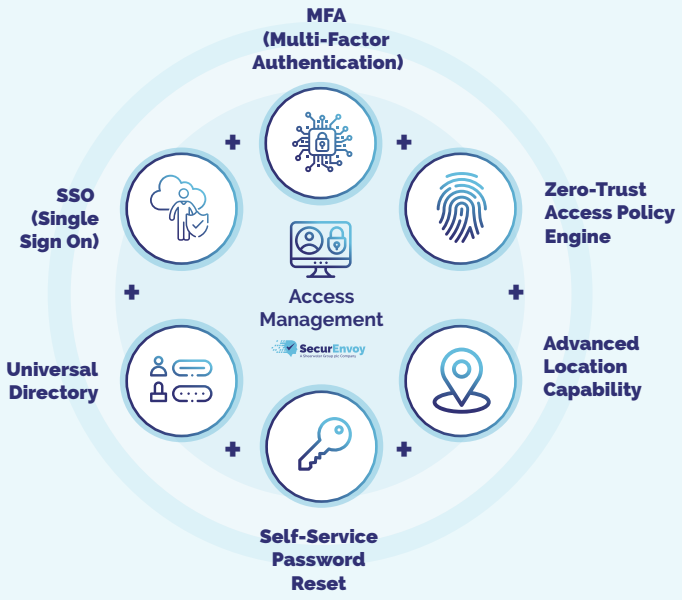
Multi-Factor Authentication (MFA)

Choose from a diverse array of authentication mechanisms, with the flexibility to align them with your organisation's specific security requirements. You can harness the power of existing devices, including mobile phones, tablets, and desktops, by Utilising software tokens or SMS-based authentication. Alternatively, consider deploying hardware tokens such as OTP (One-Time Password) or USB tokens, including support for Yubico Yubikey. This breadth of choices empowers organisations to tailor their authentication strategies precisely to their needs, ensuring a robust and adaptable Access Management solution.

Single Sign-On (SSO)

User experience can be further enhanced and productivity increased by enabling seamless single sign-on (SSO) to cloud applications.

SecurEnvoy's Access Management Solution - key features



Centralised Control and Access

- Universal Directory
- SSO

Application Integration

- Dynamic Application On-Boarding
- Legacy Applications

Authentication for a Range of Scenarios

- Conditional Access
- Authentication Options
- Passwordless
- Advanced Location Capability

Easy Administration, Reporting and Customisation

- Self-Service Password Reset
- User Access Reporting
- Customisation

The Capabilities of SecurEnvoy On-Premise Access Management (Contd.)

Conditional Access Policy Engine

Harnessing the capabilities of the sophisticated conditional access policy engine empowers organisations to embrace the principles of zero trust, enabling meticulous control over access to corporate assets. By crafting stringent access protocols, organisations can tightly govern entry, ensuring that only authorised individuals gain access to the specific resources they require. This approach aligns seamlessly with the ethos of zero trust, reinforcing security while enhancing access management.

Advanced Location Awareness

To enhance security, the SecurEnvoy Access Management solution offers the capability to establish authentication safe zones, meticulously controlled not only by Geo-IP but also bolstered by GPS technology for enhanced precision. Specific geographic regions can be designated as approved access locations. Access is granted only if the mobile push authentication confirms the user's presence within the designated safe zone. Conversely, if the user is located beyond the configured location radius, access will be promptly denied. In scenarios where data sovereignty and access assurance are of the utmost importance, this feature assumes a critical role.

Integration with Legacy Technologies

Established organisations, with a history spanning several years, often find themselves managing a hybrid environment comprising modern applications supporting authentication protocols like SAML, alongside legacy technologies that rely on RADIUS authentication. SecurEnvoy's Access Management solution adeptly addresses this challenge by seamlessly integrating a comprehensive RADIUS server into its offerings. This integration empowers organisations to exercise granular control over access, especially for technologies such as IPSEC and SSL VPN, facilitating a cohesive approach to authentication across diverse systems.

Secure Remote Desktop Protocol (RDP) & Console Access

The security of Windows Servers and Desktops, including both physical and virtual RDP connections, can be significantly fortified through the implementation of Multi-Factor Authentication (MFA). This can be achieved by deploying the SecurEnvoy Windows Logon Agent, an integral component of the SecurEnvoy Access Management Solution. When combined with the Conditional Access Policy engine rules, this solution empowers organisations to establish stringent access controls based on location, time, and LDAP group memberships, thus enhancing overall security and governance.

More information on Windows Logon Agent can be found in this whitepaper >

10 Key Benefits of Access Management deployed on-premise

1. Enhanced control and sovereignty over sensitive data.
2. Customised access policies aligned with unique business needs.
3. Greater security through direct oversight of infrastructure.
4. Compliance adherence, meeting regulatory requirements.
5. Seamless integration with existing on-premise systems.
6. Reliable performance regardless of external network connectivity.
7. Potential for long-term cost savings.
8. Mitigation of third-party access concerns.
9. Ideal for organisations with legacy systems.
10. Supports precise data residency requirements.

Access Management Solution

Conclusion

In summary, while public SaaS/Cloud deployments of Access Management solutions offer scalability and convenience, on-premise deployments remain a valid choice in situations where data sovereignty, customisation, security, and compliance requirements take precedence.

Organisations should carefully evaluate their unique needs and regulatory obligations when deciding between these deployment options.

SecurEnvoy
A Shearwater Group plc Company

The SecurEnvoy Zero Trust Access Solution

The SecurEnvoy Zero Tust Access Solution allows organisations to provide verifiable trust in every action taken.

By providing the identity of the user, the device and the data they are working on you can monitor and prove exactly who is doing what at any time.

Let's Talk

Talk to our experts today for a No-hassle, No Obligation Consultation.

support@securenvoy.com
securenvoy.com
linkedin.com/company/securenvoy
twitter.com/securenvoy