wallix

WALLIX Guide

How to secure the Enterprise against Identity-Based Attacks



Guide: How to Secure the Enterprise Against Identity-Based Attacks

1. Introduction

Identity Security is the discipline of protecting digital identities – the accounts, credentials, and entitlements through which people, machines and services access an organisation's systems. It matters because identity has become the primary attack surface. Most breaches no longer begin with an attacker breaking through a perimeter; they begin with a stolen credential, a phished session, or an over-privileged account being quietly abused.

Credential theft and phishing remain the most common entry points, increasingly bypassing basic MFA through adversary-in-the-middle techniques. Once inside, attackers exploit excessive or dormant entitlements to move laterally and escalate privileges. And the problem is compounded by scale: non-human identities, service accounts, API keys, and machine-to-machine connections now outnumber human ones in most organisations, often unmanaged and rarely reviewed. Every unverified identity and every unnecessary entitlement is standing risk.

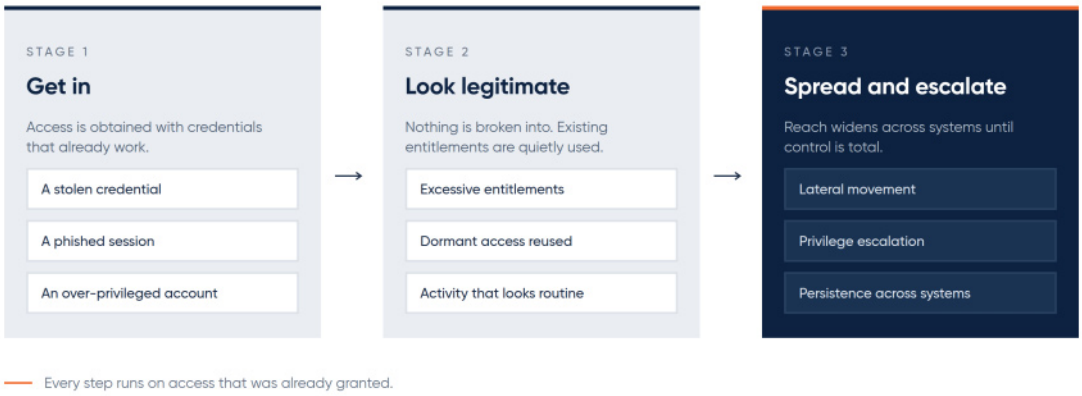


Figure 1 How an identity-based attack unfolds

If identity is where attacks begin, then controlling access is where defence must begin. This is the role of identity access: the operational layer of identity security that verifies who is connecting, enforces how they authenticate, and governs what they are entitled to do — continuously, not just at login. Before any organisation can talk

about advanced controls or governance maturity, it needs this foundation in place: strong authentication, least-privilege access, and a managed identity lifecycle from arrival to departure.

2. The Problems Organisations Face

2.1 Identity sprawl and fragmentation

Few identity landscapes are the product of deliberate design. They tend to grow over time, shaped by whatever the organisation needed at each stage: a new application here, a cloud platform there, an acquisition that arrives with its own directory and its own conventions for granting access. Years of this leave behind what is usually called identity sprawl, the same employee holding a dozen unconnected accounts, entitlements spread across systems with no awareness of each other, and no reliable way to answer a question as basic as who has access to what.

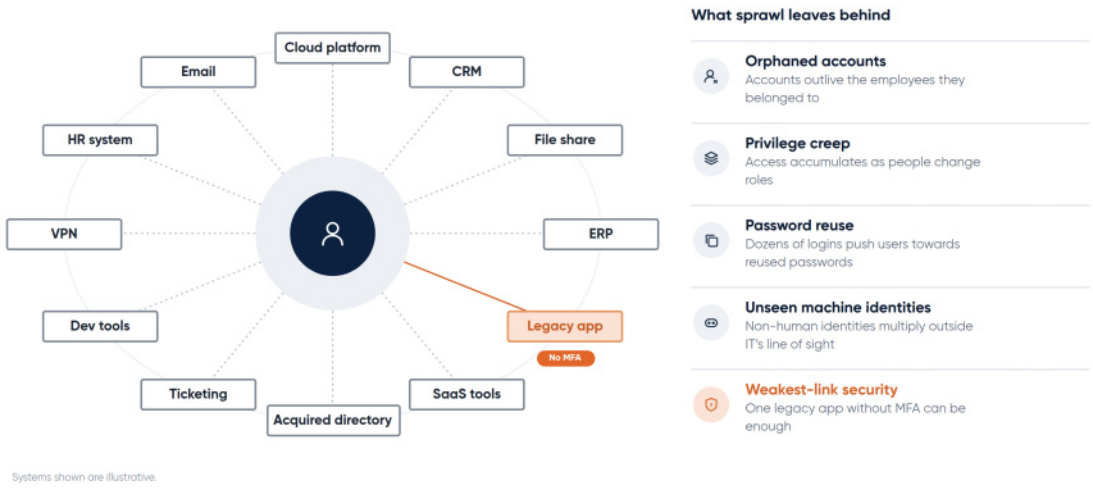


Figure 2 Identity sprawl: one employee, a dozen unconnected accounts

The risks that come with sprawl are well documented, and most of them follow from the same underlying issue: nothing is managed in one place. Deprovisioning has to happen system by system, so accounts routinely outlive the employees they belonged to. Access accumulates as people change roles, because permissions are granted when needed and seldom reviewed afterwards. Users faced with dozens of separate logins fall back on reused passwords, since no one can maintain that many strong, unique credentials. Meanwhile the population of non-human identities —

service accounts, API keys, integration credentials, **AI agents and other machine identities** — grows faster than any other, often created outside IT's line of sight and left running on static credentials for years at a time.

Fragmentation makes all of this harder to correct. Where authentication is enforced separately in each system, overall security settles at the level of the weakest implementation; a single legacy application without MFA can be enough. Where access policies sit in different consoles, keeping them consistent becomes a manual exercise, and preparing for an audit means reassembling the picture one system at a time. Security teams find themselves responsible for an attack surface they can only partially see, and the seams between systems are precisely where attackers tend to look.

It is also worth noting that sprawl rarely takes the same shape twice. Most environments are hybrid out of necessity, combining cloud applications with on-premises infrastructure — and in regulated or sovereignty-conscious sectors, with systems that cannot leave the organisation's own perimeter at all. A serious response to identity fragmentation has to account for the whole of that landscape, not only the parts that are easiest to connect.

2.2 Credential attacks have industrialised

Phishing is no longer a small-scale or highly specialised activity. Phishing-as-a-service platforms provide attackers with ready-made infrastructure for imitating corporate sign-in pages, collecting credentials, and bypassing some commonly deployed forms of multi-factor authentication. Services such as Tycoon 2FA have enabled these capabilities to be used at scale, lowering the technical barrier for attackers and turning advanced phishing techniques into commercially available services.

A particularly significant development is adversary-in-the-middle phishing. In an AiTM attack, the attacker places a proxy between the user and the legitimate authentication service. The victim completes the genuine sign-in process, including any one-time code or push approval, while the attacker captures the resulting session token or cookie. This can allow the attacker to access the account without repeating the authentication process, even where conventional MFA is enabled. Microsoft reported a 146% increase in observed AiTM phishing attacks during 2024.



Figure 3 Anatomy of an adversary-in-the-middle attack: MFA is completed, and still bypassed

Other forms of MFA also have limitations. Push notifications may be exploited through repeated approval requests, while one-time passwords can be intercepted or relayed in real time. The relevant question is therefore not simply whether MFA is present, but whether the authentication method is resistant to phishing. Methods that rely on shared secrets, codes, or user approval provide materially different protection from cryptographic methods such as FIDO2 security keys and passkeys.

Credential abuse nevertheless remains an important route into corporate environments. Verizon's 2026 Data Breach Investigations Report found that stolen credentials accounted for 13% of observed initial-access activity. Once attackers gain access through a legitimate identity, their actions may initially resemble those of an authorised user, making suspicious activity harder to distinguish from normal behaviour.

2.3 Regulatory pressure

Regulators across every major market are converging on the same expectation: organisations must be able to demonstrate control over who has access to their systems and prove it. In Europe, NIS2 expands cybersecurity obligations across more sectors. It includes access control and multi-factor authentication among the measures covered entities may need to implement. At the same time, DORA requires financial entities to strengthen governance of ICT risk — including access controls, privileged accounts, and third-party access. GDPR continues to require appropriate protection of personal data, making documented access governance, regular permission reviews, and timely account removal important compliance controls.

The pattern repeats well beyond Europe. In the US, SOX and HIPAA require demonstrable access controls in their sectors, and federal zero-trust directives are pushing agencies and suppliers towards phishing-resistant MFA. The UK pairs its retained GDPR with FCA operational resilience rules and Cyber Essentials, which makes access control and MFA a condition of much public-sector business. Across the Middle East, data protection laws like Saudi Arabia's PDPL are maturing fast, with regulators such as SAMA setting explicit identity requirements for finance. Asia-Pacific follows the same arc, from Japan's APPI and Singapore's PDPA to MAS guidelines on privileged access. And above the national layer, PCI DSS and ISO 27001 travel with business itself, making access management a contractual expectation as much as a regulatory one.



Figure 4 Different frameworks, one shared expectation

Individually, each framework has its own scope and timeline. Taken together, they point in one direction: identity and access controls are no longer an internal security preference but an external obligation — one that organisations must be able to evidence on demand.

2.4 The user-experience trap

Lastly, security controls that create excessive friction are often bypassed. Frequent authentication prompts encourage users to seek shortcuts. Complex password requirements lead to reuse, predictable variations, and insecure storage. Slow access-request processes increase the likelihood of shared credentials or unmanaged workarounds.

This is not simply a question of user discipline; it is a design problem. Workforce access security is most effective when the secure path is also the easiest one. Users should be able to authenticate once, access the applications required for their role, use factors that are faster and safer than passwords, and resolve routine access needs without unnecessary delay. A solution that treats usability as secondary will eventually create the behaviours it was intended to prevent.

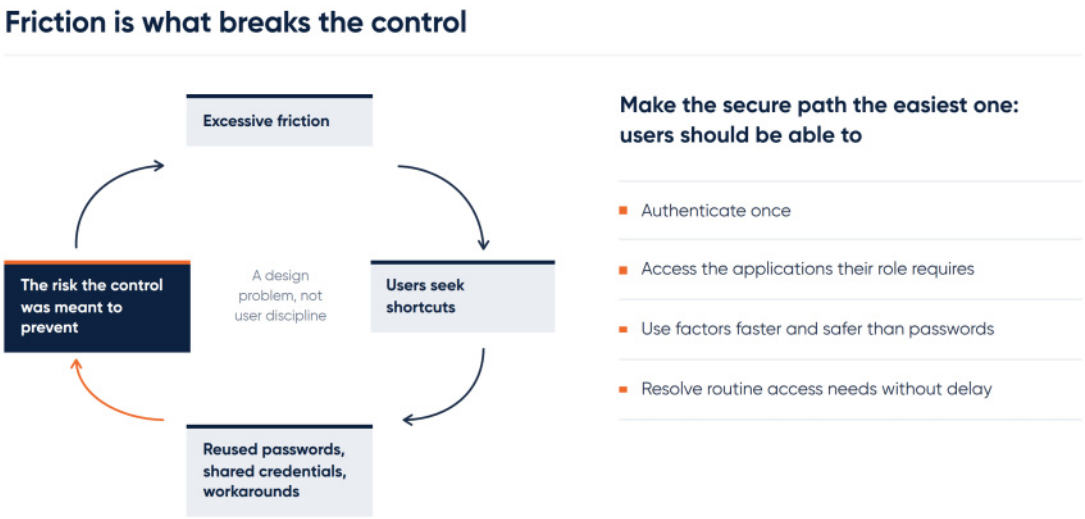


Figure 5 Friction creates the behaviour it was meant to prevent, so design it out

3. Where the Pressure Is Highest

These challenges affect most organisations, but they are particularly acute in sectors that combine complex environments, sensitive systems, and demanding regulatory requirements.

Public sector and government

Public administrations operate large and heterogeneous application estates, ranging from modern cloud services to systems that have been in use for decades. These systems are accessed across ministries, agencies, and local authorities, often under strict requirements for auditability, sovereignty, and control over where identity data is stored.

For these organisations, the priority is to provide consistent authentication across the full application estate, introduce strong factors according to applicable public-sector requirements, and maintain complete evidence of access activity under the organisation's control.

Critical infrastructure and industry

Energy, transport, water, manufacturing, and other industrial operators must secure environments in which availability is essential. They may operate segregated operational technology networks, remote sites with limited connectivity, and legacy systems that cannot easily be replaced or modified.

Authentication in these environments must remain reliable without depending entirely on external services. It must also integrate with existing industrial and legacy systems while generating the records required for audit and regulatory oversight. The objective is consistent workforce authentication across offices, plants, and remote sites without introducing an unacceptable operational dependency.

Financial services

Financial institutions operate under extensive requirements for ICT risk management, resilience, and third-party oversight. Employees, contractors, service providers, and technology partners may all require controlled access to sensitive systems.

An effective approach must account for every identity, enforce appropriate authentication, restrict and monitor privileged and third-party access, and make evidence available when required. The focus is not only on preventing unauthorised access but also on demonstrating that access is governed continuously.

Healthcare

Healthcare environments combine highly sensitive personal data with workflows in which delays can affect patient care. Clinicians may move between locations, use shared workstations, and require rapid access to multiple clinical systems.

Authentication must therefore be fast enough to support clinical work while ensuring that access to patient information remains controlled, attributable, and auditable. The goal is not to choose between usability and security, but to design access controls that support both.

4. What an Identity Access Solution Must Do

An effective workforce access solution should provide five core capabilities.



Figure 6 Five core capabilities of a workforce access solution

4.1 Single, seamless access across the application estate

The foundation is single sign-on across cloud, and on-premises. Users authenticate through a consistent access point and reach the applications authorised for their role without maintaining a separate password for each one.

This reduces the number of credentials in circulation, lowers password-reset demand, and gives IT teams a clearer point from which to apply policy and monitor access. It also shifts more importance onto the central authentication layer. Because that layer protects access to multiple applications, it must be strongly secured, highly available, and closely monitored.

4.2 Authentication that resists modern attacks

Multi-factor authentication requires users to present factors from different categories, such as something they know, something they possess, or something they are. This makes account compromise more difficult, but the level of protection depends heavily on the factors used.

One-time passwords can be intercepted or relayed. Push notifications may be approved after repeated prompts or social engineering. Adversary-in-the-middle attacks can proxy a legitimate authentication session and capture the resulting session token, even when some forms of MFA are enabled. The presence of MFA alone therefore does not guarantee resistance to phishing.

Phishing-resistant authentication addresses this weakness. FIDO2 and WebAuthn methods, including hardware security keys and passkeys, bind authentication to the legitimate service through public-key cryptography. There is no reusable code or

into processes across HR, IT, and security. A workforce access solution that demands migrating away from this foundation fails before evaluation begins.

The requirement is federation: the solution sits on existing directories as the authoritative identity sources, synchronises with them, and extends their reach to applications through standard protocols, SAML and OpenID Connect for modern web applications, RADIUS for network equipment and infrastructure, with SCIM for automated user provisioning to compatible services. Existing identities, groups, and organisational logic carry over intact; the application estate, including systems that were never designed for federation, becomes reachable through one authentication layer.

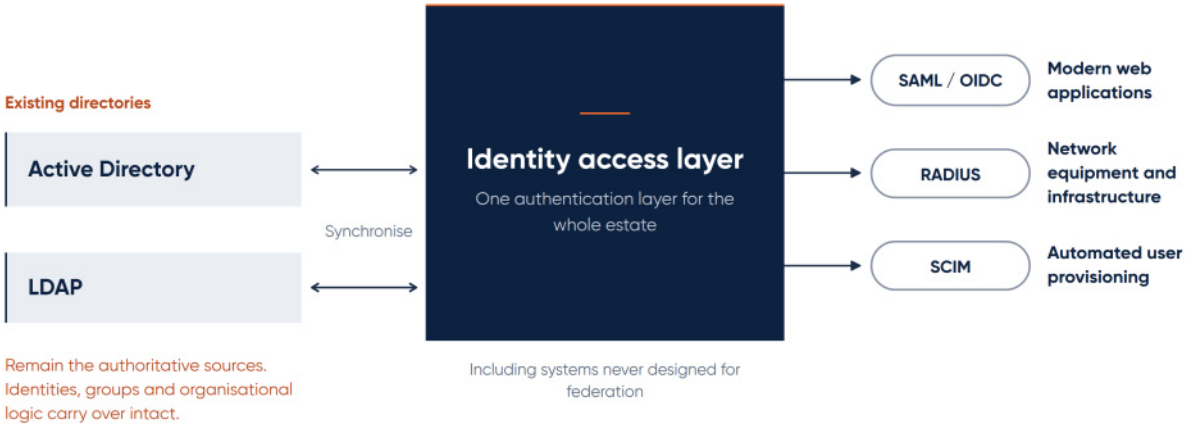


Figure 8 Federation extends the directories you already have, through standard protocols

This is also what makes deployment realistic on compliance timelines. Mandates with fixed deadlines do not leave room for multi-year directory migrations; a solution that layers onto current infrastructure can enforce strong authentication across the estate in months.

4.4 Identity lifecycle without the manual burden

Every identity has a lifecycle, arrival, role changes, departure, and every stage is a point where access can silently diverge from what it should be. The solution must make the lifecycle administrable from one place: accounts created with role-appropriate access from day one, permissions adjusted as roles change, and departure revoking access everywhere at once. Group- and role-based policy, applied centrally, replaces per-application administration.

This closes the two chronic failure modes of manual administration: privilege creep, and orphaned accounts that survive their owners' departure. It also converts a recurring operational cost into a governed process, the access a person holds is the access their role defines, demonstrably and at any moment.

4.5 Audit evidence, built in

Every regulation discussed in this paper converges on the same questions: who has access to what, how is that access protected, and can you prove it? A workforce access solution must answer from its own records: complete authentication logs, a live map of user-to-application entitlements, and reporting suitable for auditors rather than only for administrators. Integration with SIEM platforms carries identity events into the organisation's broader detection and response capability.

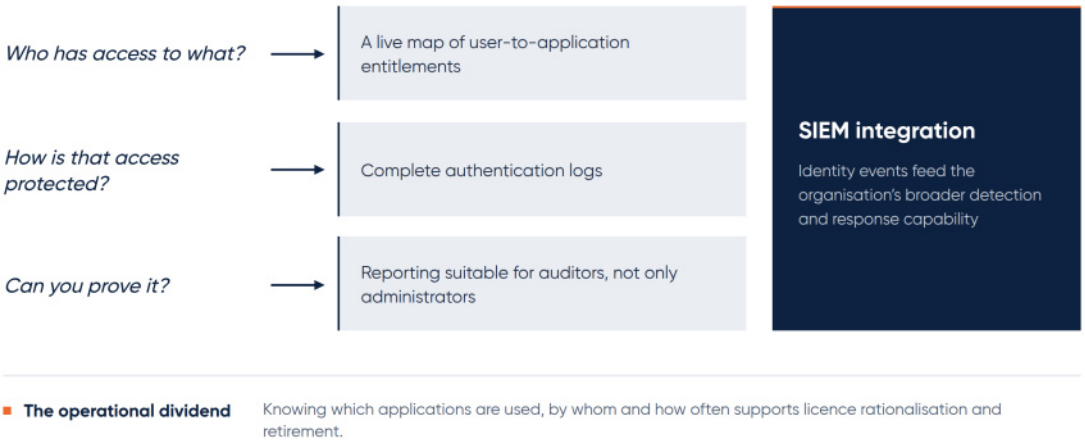


Figure 9 The auditor's three questions, answered from the solution's own records

Beyond compliance, this visibility has an operational dividend: knowing which applications are actually used, by whom, and how often gives IT teams the evidence to rationalise licensing and retire what the organisation has outgrown.

5. One Platform, Your Deployment Model

The capabilities above define *what* a workforce access solution must do. Where it runs is a separate decision — one that depends on the organisation's regulatory context, infrastructure, and risk posture rather than on the capabilities themselves.

As a service (SaaS). The fastest path to capability: no infrastructure to provision, operations and updates handled by the vendor, scaling handled transparently. Built for organisations that want workforce access security running in weeks and prefer to consume it rather than operate it.

As an on-premise appliance. The same capabilities, deployed within the organisation's own infrastructure. Identity data, authentication flows, and logs remain entirely under the organisation's control — inside its perimeter, its jurisdiction, and its operational responsibility. Built for organisations with sovereignty requirements, regulated tenders that preclude cloud-delivered identity, and environments, industrial, air-gapped, connectivity-constrained, where authentication must function with no external dependency.

Two questions decide the model. *Where must identity data live?* If regulation, policy, or the sensitivity of operations requires identity to remain under direct organisational control, the appliance answers structurally what contractual assurances answer only partially. *What must authentication survive?* If the environment must keep operating through loss of external connectivity, a plant, a ship, a classified network, authentication cannot depend on a cloud service being reachable.

Neither model is a compromise. They are two deployments of one platform, and the right choice is the one the organisation's environment has already made.

6. WALLIX Sovereign Identity Access

Our solution delivers Identity Security as described in this paper: single sign-on across applications; multi-factor authentication including phishing-resistant methods; user synchronisation and identity federation with existing Microsoft Entra ID, Google Workspace, Active Directory and LDAP environments; delegated authentication to target applications; centralised lifecycle administration; and complete audit visibility. It is available as a service or as an on-premises appliance, with the same capability set governed the same way.

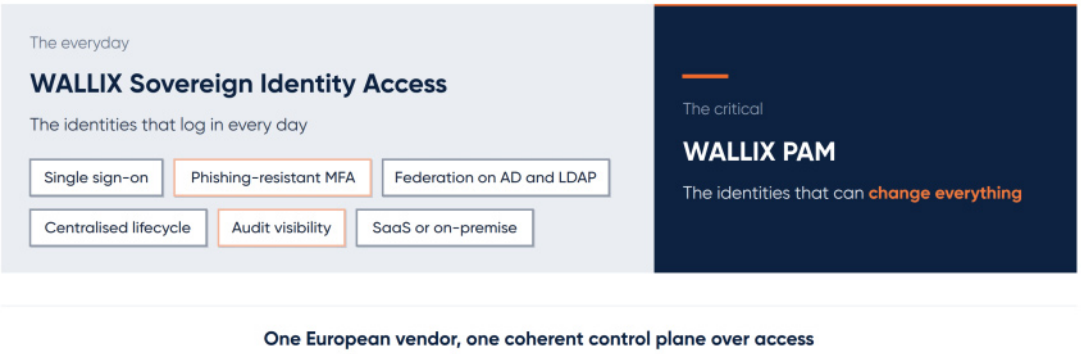


Figure 10 Two halves of one problem

WALLIX Sovereign Identity Access is part of the WALLIX platform, alongside WALLIX PAM. Identity security and privileged access are two halves of one problem, the identities that log in every day, and the identities that can change everything, and securing them through one European vendor gives organisations a single, coherent control plane over access, from the everyday to the critical.

7. Conclusion

Identity access is where the modern organisation is won or lost: it is how work happens and how breaches begin. The organisations that secure it share an approach: identity centralised rather than scattered, authentication that phishing cannot defeat, existing infrastructure extended rather than replaced, and evidence of control available on demand.

The capabilities exist. The regulatory deadlines are set. What remains is the decision to treat workforce access as the security perimeter it has already become, and to deploy that control wherever the organisation needs it to run.

about WALLIX

WALLIX (Euronext: ALLIX since 2015) is a cybersecurity vendor, European leader in privileged access management (PAM), helping organisations secure their freedom and shape their digital autonomy. The technological excellence of the WALLIX One platform, recognized by the most prestigious analyst firms, supports up to 4,000 organisations worldwide with a clear mission: to protect Identities, Access, and Privileges across IT and OT environments, combining efficiency, simplicity and compliance to help businesses evolve freely and securely in a more secure digital world.

WWW.WALLIX.COM

wallix