Security and Identity management: combating orphan and inactive accounts

formind netwrix

What is the one thing that all CIOs and IAM managers – from every sector and size of company or turnover – have in common?

Employees or external service providers will leave behind multiple open accounts once they've left the business, been promoted, or moved to another role. This phenomenon of so-called dormant (or orphan) accounts is a real threat regarding the uncontrolled cost of software licenses and online services and the significant cyber-attack surface that it creates. This lack of lifecycle management for both standard and privileged user accounts remains a real challenge for organizations and IT departments because it is the leading cause of the proliferation of orphan accounts.

But before we go any further, what exactly is **an orphan account**?

An orphan account is a technical or application account with or without privileges that is not associated with any active or existing identity.

The presence of orphan accounts is dangerous for an information system, and identifying these 'phantom' accounts can considerably reduce the IT budget allocated to systems and technological services. Without being able to locate the phantom accounts, these are the possible scenarios that a business might be exposed to:

Identity and authorisation management	• Complex rights and access management with "false" or difficult-to-conduct audits; • Reduced visibility on who has access to what, why, and since when.
Cybersecurity	• A 'no man's land' which is an easy target for cyber attackers; • Contamination of the network; • The spread of a Shadow IT mentality in the company, which increases cybersecurity risks and vulnerabilities.
Licenses and costs	• An increase in the number of ticket requests to de-provision these incorrectly active accounts; • An increase in employee onboarding time due to a lack of available licenses (which are blocked on phantom accounts), leading to a general loss of productivity; • A surplus of the IT budget for monitoring, controlling, and managing licenses ; • Time-consuming and often manual processes for releasing unused licenses.
Digital Responsibility and GDPR	• Failure to adopt a responsible digital approach; • Legal problems if contracts are violated; • Non-compliance with GDPR if these accounts were to be misused by other users.

The list in the table above is not intended to be exhaustive. Having identified the main issues, **how can you prevent orphan accounts from appearing in your information system in the first place?**

The proliferation of these accounts is due mainly to incomplete or non-existent management of the identity life cycle, which impacts the access and authorization lifecycle. A direct link between the status of identity and the automatic calculation of resource allocation, backed up by frequent synchronization with the target systems, allows this holistic and comprehensive vision and governance to contain the emergence of orphan accounts at the source.

An Identity and Access Management (IAM) solution with a flexible and structured architecture makes it possible to easily cover all joiners, movers & leavers within the organization, whether it is:d'un départ programmé après lequel il faudra garantir la suspension puis le retrait des rôles et le dé-provisionnement de l'ensemble des comptes, en gérant une période de grâce éventuelle,

- A scheduled departure, after which the suspension and withdrawal of roles and the de-provisioning of all accounts must be guaranteed while managing a possible grace period
- Immediate departure;
- A long-term suspension;
- Internal reorganizations;
- The management of multiple positions and functions, which can quickly become complex.

The architecture of the Netwrix Usercube solution natively meets this need to distinguish between the employee's digital identity and their IT resources (in particular, multiple accounts assigned to them).

Netwrix Usercube provides a clear distinction between identities and their rights and the technical resources that manage these within the information system.

The Netwrix IGA (Identity Governance & Administration) solution was designed from the outset to manage an organization's digital identities and the rights necessary to achieve its goals. Netwrix Usercube clearly separates the identity and its rights and the technical resources that must be allocated to it in the information system in connection with these roles. These technical resources take the form of connection accounts (allowing access to different systems and applications) and specific rights that can occur, for example, by the attachment of a connection account to an Active Directory group (or LDAP or Entra ID) or by assignment to an application profile within an application.

By managing the life cycle of the identity (arrival, departure, transfer, multiple assignments, extended leave of absence, change of contract, etc.), our solution can – in every situation – provide the identity with the resources it needs for its role. Still, it can also remove them as the situation changes.

Netwrix Usercube, through its connectors, automatically discovers the accounts in your information system and allows them to be linked to identities. In this way, orphaned accounts are immediately exposed and can be dealt with.

For Netwrix Usercube, a digital identity is a person or thing that needs to interact with the information system. People (internal or external to the company), but also applications (which may require service accounts to access certain IT resources), connected objects (IoT, connected meeting room, etc.), and bots (RPA) are also managed. By covering all digital identities and managing the associated connection accounts, our IGA guarantees the management of all the company's accounts and the lifecycle related to identities.

Netwrix Usercube is an IT control tower that detects any discrepancy between the required rights defined in its repository and what it finds in the information systems. These discrepancies can then be addressed, whether technically by requesting the deletion of accounts directly in the solution but also functionally by identifying any areas of improvement needed by the organization (communication, training, change).

In addition to accounts and identities, Netwrix Usercube also effectively manages the rights assigned to these identities, but this will be the subject of a future discussion.

The Formind x Netwrix partnership

Formind and Netwrix, partners for years and key players in the French market, work together on projects with companies and organizations in various sectors such as banking, insurance, industry, and energy.

Formind has leading IAM expertise – both functionally and technically – enabling us to offer our clients the best solutions for their specific needs.

Combining the two companies can deliver a unique value proposition that matches your project and expectations.

About Netwrix Corporation

Cybersecurity that works for you

Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

For more information, visit www.netwrix.fr

Formind

Security for Business Performance

Formind is a French independent leader and a pure player in cybersecurity. PASSI-qualified, in the process of being PRIS-qualified and ISO 27001-certified, Formind helps its customers to be more resilient and to protect themselves from cybersecurity risks thanks to its three pillars: ADVISORY – INTEGRATION – SOC&CERT
Formind also developed a dedicated offering for small and medium-sized businesses, addressing their specific cybersecurity issues.

For more information, visit www.formind.fr or contact@formind.fr