IDENTITY GOVERNANCE AS NOWADAYS' NECESSITY

JANUARY 2020

WHITE PAPER

Content

Introduction

Many organizations are experiencing challenging situations on the market. Sometimes they even lose their position against the competition due to lack of efficiency. To keep up with the speed of market evolution, the organization's internal processes have to be seamless and potential threats need to be minimized.

In the world of identity management and identity governance the rules are the same. The organization using up to date quality and inovative technology has a bigger potential to get a competitive advantage. This means a solution which can ensure security and protection of information as well as automation of the processes. There are many solutions dealing with identity management and also many taking care of identity governance. But in the context of efficiency and automation, why not to have both in one solution?

Two in one

The quality of identities managing solution relates from various technological aspects which determine what value the solution will be able to bring. However, there are also another requirements the organizations find necessary to meet: the business ones. There can be requirements such as speeding up IT processes, automation or call center efficiency but also regulatory compliance, information security or efficient organizational management. The solution should be useful for both user groups: IT administrators as well as managers, security officers or auditors.

Most solutions dispose with two different products which cover the technological and business needs of the organizations separately by means of identity management and identity governance. They very often originate in various environments, use different technologies and are put together only by a series of acquisitions. Considering the huge overlap of identity management and governance concepts altogether with the requisition of their close cooperation, an integration of these products is often very problematic.

Subsequently, the deployment as well as long-term maintenance of such a solution can be very complicated. And in the end, the organization can easily find itself in a costly situation, stuck in trials of resolving occuring problems and not working effictively even by a chance. The answer to such serious problems is a complete solution covering identity management and identity governance (frequently called identity governance and administration) in one product, where these two parts work seamlessly together.

Security during whole user's lifecycle

The organization is able to limit potential threats with appropriate control over processes. Identity governance and administration (IGA) provides an ability to define, enforce, review and audit important policies. This can be done any time during user lifecycle, from onboarding new users to their offboard and the elimination of their accounts.

When new employe is hired, he needs to get his roles and accesses assigned as soon as possible so there is no time wasted and he can proceed to work immediately. Also when his position changes or some employees are added to a working group, a reorganization of accesses or passwords needs to be fast. From the IGA point of view, it is also inevitable to do regular access reviews and audits. If an employee leaves the organization, his accounts and access privileges have to be disallowed as soon as possible to avoid any potential security exposures.

The organization may also need to grant access to customers, business partners or suppliers and provide secure access to externally hosted applications such as cloud-based ones. Offboarding partners is also a common thing in business which can become complicated. In connection with that, there is a need for the coordination of authentication and authorization with the company's back-end or third-party systems.

In case of all these actions, an identity governance and administration tool as a part of complete solution can satisfy all organization's needs. It can help with reducing the risk of fraud, theft of intellectual property or data loss. It will also help to save time as well as costs and increase efficiency.

Use case: enforcing security policy

An international telco organization operating in Europe, Asia, Africa and Oceania has teams consisting of internal employees as well as partners and suppliers. As a prevention from potential threats the organization defines its security policy. The security policy then needs to be applied and enforced consistently over many applications, platforms, operating system and devices. However, in large organizations with heterogeneous environment it is almost impossible to enforce it without appropriate tooling.

Enforcing rules such as disabling employee's accounts after he leaves the organization may look simple at the first sight. But aspects like identifying all his accounts and usernames make this action complex as such list is usually not maintained anywhere. A leaving employee is a serious security risk as he accumulated enormous access privileges over the time. His accounts must be disabled successfully: the systems may be restored from backup, which may enable previously disabled accounts or human error can occur. When the number of identities grows beyond few thousands and there's few dozens of target systems, it becomes a serious threat.

The situation is even more complex, as both security policy and user population are moving targets. The security policy must adapt to legislation, regulations and changes in business environment. The user population is changing all the time, there is employee fluctuation, reassignment or reorganization as the organization keeps moving constantly.

To minimize such security risks and maximize efficiency the organization needs automation. Identity management systems provide automation of basic identity maintenance while identity governance systems automate the high-level maintenance of roles, privileges, segregation of duties or compliance. These systems need a feedback mechanism to be of any practical use and not to fail. Only then the identity management and governance system have precise and up-to-date information about security-sensitive aspects of all applications. This way the solution is complete and able to provide high efficiency as well as lower the security risks.

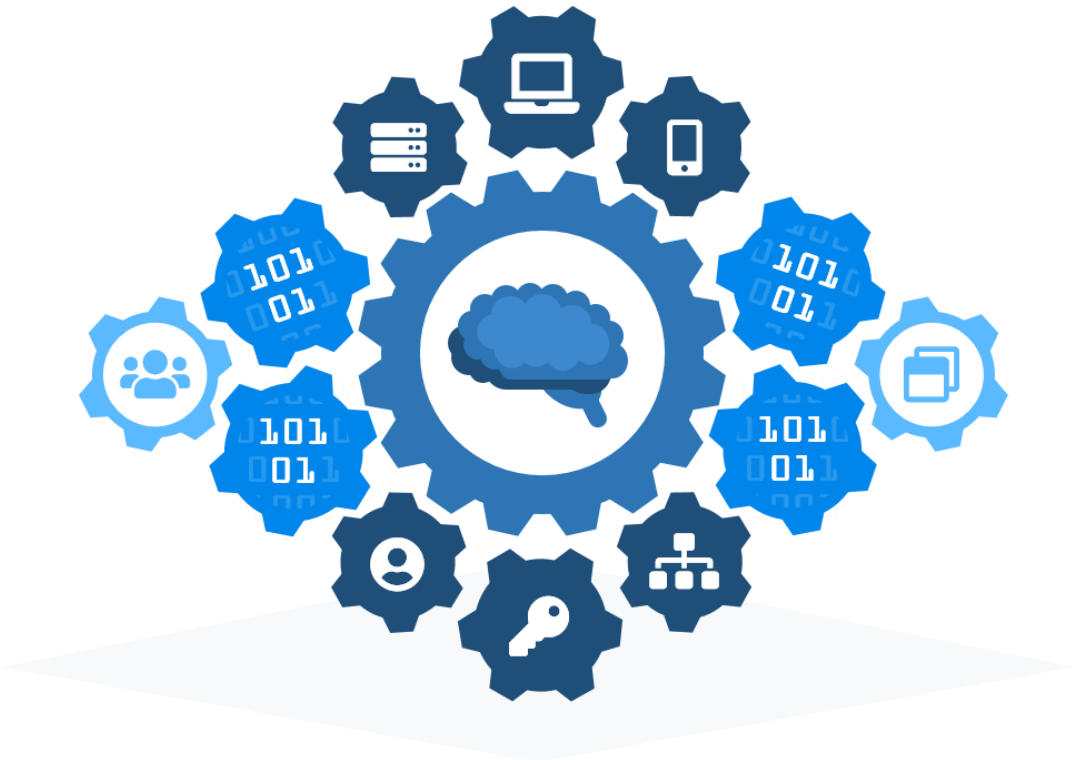
There is an identity governance solution that can help the organization to deal with all these problems: midPoint. From its very beginning midPoint was designed as a unified identity management and governance platform. While low-level identity management and synchronization are part of MidPoint's basic capabilities, it is designed to handle also high-level identity governance tasks. Both high-level and low-level capabilities are provided in a unified system that is naturally integrated.

A complete solution

MidPoint is open identity & organization management and governance platform. It is a complete solution which covers both technological and business requirements of the organization by means of identity management and identity governance. MidPoint is a slick product with a single all-encompasing architectural design that combines both identity management and governance features using a common data model. This approach is a huge difference for a long-term maintenance of the solution.

MidPoint is a unique product designed to handle broad range of deployments. With midPoint the organization can start small with simple identity management deployment and gradually evolve the solution to support complex identity governance scenarios. The process is seamless and evolutionary, therefore it provides business continuity and excellent investment protection.

There is no security without good identity management, that's why midPoint disposes with ITSM integration feature. Many identity management systems have such capability, but usually only as a one-way communication. However, a system without feedback means potential threat and security risk. For instance without feedback it may easily happen that accounts of a leaving employee remain enabled. MidPoint has an ability to implement the feedback channel for manual fulfilment and prevent the organization from serious security problems.



As for midPoint being a complete solution providing both identity management and identity governance features, it minimizes the risks of potential complications caused by integration trials of the products from different environments. MidPoint keeps the organization secure thanks to high level of automation as well as well-developed feedback mechanism. It is nowadays one of the rare breed of systems supporting a state-of-the-art identity management and fair deal of identity governance in the same product. MidPoint provides the security and efficiency to many organizations all around the world.

For more information

To learn more about midPoint and ways it can be useful to the organizations, please visit our site evolveum.com or write us an email.

About Evolveum

Evolveum is an open company with rich experience in the field since 2000. With its high development performance Evolveum constantly works on improvement of its identity & organization management and governance platform midPoint. This progress of midPoint is covered by its numerous releases which helped to meet the needs of the clients. Nowadays Evolveum focuses on enhancement of midPoint's governance feature, organization management and management of user roles to keep up with clients' growing requirements. The company's future vision is to keep its clients technically up to date as well as offer a platform always capable to solve clients' business problems.