Identity & Access Management –

Stay one step ahead of identity theft in your company

CHAKRAY

About this guide:

This guide is intended for IT managers, CIOs and executives who need an identity & access management solution.

Identity & Access Management

User access and identity in companies have become some of the most important digital assets. Identity management and the access role acquisition process are some of the most pressing subjects among major company CIOs.

HP Inc. President Helena Herrero (2017) highlights how many IT managers focus exclusively on the safety of computers, servers and mobile devices - a formula that is increasingly becoming obsolete. This is because the new gateway for cyberattacks is targeted at connected devices, mainly affecting those that are within the scope of the Internet of Things (IoT).

In this guide we will discuss the most relevant issues of **Identity & Access Management** (IAM): the current digital security landscape, the challenges faced by IT managers and the way in which interrelated solutions work.

This guide is intended for IT managers, CIOs and executives who need an identity & access management solution.

Table of contents

1. The Landscape

For over a decade, technology has been transformed by a growing expansion rate. In the 80s, only a few users had the privilege of having access to computers. But during the following years, access kept expanding and companies started owning more computers and more computer systems.

Data management in systems and business processes resulted in the need to rethink access to such systems. Information safety and data safeguarding became a critical issue within organizations.

It is at that moment when regulations by governments and security standards by companies emerged for the protection of data

1.1 The digital security market

When faced with an imminent digital transformation and having to migrate their critical business applications to the cloud, many companies are filled with doubt and hesitant in regard to the security of these management models.

Guaranteeing data and identity security is one of companies' greatest concerns, especially due to the key business information they may harbor. In addition, a new European Data Protection Regulation affects any company working with any EU country.

Gartner, a consulting firm specialized in information technologies, forecasted that cloud-based security services would increase by 21% in 2017, reaching the overall value of 9 billion dollars by 2020. As attackers improve their strategies and thefts, companies will need to stay updated and improve their security capabilities. Hence the growth of the digital security market.

> *“Gartner, a consulting firm specialized in information technologies, forecasted that cloud-based security services would increase by 21% in 2017, reaching the overall value of 9 billion dollars by 2020.”*

This means that CIOs and IT managers are the leaders of company system security. They should be committed with the constant evaluation of company security levels and stay up-to-date on the latest technology.

For advanced attacks, prepare with the right technology

2.2 Cloud security

In 2016, over 160 major security breaches took place involving major Spanish companies. This resulted in a 9.5 million dollar expense (Dealerworld, 2017). Today more than ever it is necessary to protect connected devices and identities used by people to access various applications. Furthermore, one of the main problems faced by executives is that the attack vector transforms and changes rapidly.

> “*In 2016, over 160 major security breaches took place involving major Spanish companies.*”

Migration to the cloud is now a reality, which leads to a growing demand for increasing security levels in that realm. It is for this reason that it is becoming one of the markets that sees great opportunities.

Three facts that lead companies to review their security:

- Vertiginous growth of cyberattacks targeting companies
- Data theft
- Rise in vulnerabilities

2.3 Small & Medium-sized enterprises under threat

One of the myths of the world of digital security is that cyberattacks only happen to large organizations. But this is not entirely true, because the security market has been propelled by small & medium-sized companies.

In 2017, cloud-based services aim to attain a growth of 5.9 billion dollars worldwide according to Gartner. According to the Dealerworld specialized magazine, this data is quite significant, since it would place the cloud security market over the total information security market.

Another major item worth noting is that recently created companies, such as SMEs or start-ups, require agile solutions with simplified features. The seek solutions with attractive delivery models that offer the right security for their business models.

We can list three key factors why company concern over cloud security is on the rise:

- Corporate security threats are increasing
- Company personnel require improvements in management services
- Greater operational and cost benefits

2.3 Digital security trends

Analysts foresee that the main Cloud-based security service niches with the highest rate of success and scalability are Security Information and Event Management (SIEM) and **Identity Access Management** (IAM), as **emerging technologies.**

SIEM is a technology that combines two different security products: SIM (Security Information Management) and SEM (Security Event Manager). This solution analyzes and prioritizes security events within the network. It thereby provides a real-time analysis of security alerts generated by the network's hardware and software.

IAM, which is this guide's main subject, is a technology that is used to automate user identity management and access permissions.

Experts point out that emerging services such as SIEM and IAM offer companies a very significant potential for growth. However, it should be noted that according to forecasts by Gartner, products comprised within the scope of **Identity Access Management** will see the greatest growth within the next 3 years.

IAM is a technology product that falls within the scope of Identity & Access Management as a service (IDaaS).

2. The challenge

It is common to find that when everything is working, IT departments are not taken into account, but when something goes wrong, these departments are at the eye of the storm.

2.1 Challenge for the CIO

Grave issues that may occur, such as downtime in a technological service, are usually tackled first. These issues go hand-in-hand with a loss of trust by the company in IT services. It therefore becomes a main concern for CIOs: trust in the services provided.

Additionally, one should add that the most common problem faced by IT personnel is, in particular, the management of password-based identities and user access privileges.

Companies are currently using multiple systems. These systems have a myriad of users and identities that translate into multiple passwords and various privileges. Moreover, they are managed by various processes involving additions, deletions and changes, and they also need to be operational 24/7.

According to the Halock consulting firm each person has an average of 25 accounts across different systems, which keeps growing with each new service and app that appears on the market. This phenomenon is dubbed identity sprawl by experts, and when added to the various internal identities in a company, the outlook is confusing at best. Furthermore, this identity sprawl is simplified by the fact that people have many identities but only a few passwords to manage them. It seems like a great opportunity for hackers to attack organizations on this front.

Handling these incidents takes time, resources, and results in direct expenses for IT departments, which impacts the company's productivity.

2.2 Loss of productivity and quality

If management is not focused on addressing the complexity of the various systems and different internal flows of information for the management of user data, variability is introduced into company processes.

This variability makes processes lose their meaning and lead to diminishing quality and productivity. This is compounded by the fact that users want immediate service, and even more so in regard to user addition, deletion and modification. According to Gartner, resetting of accounts encompasses 30% of Help Desk calls.

These incidents lead to a perception of inefficiency by the IT department, unfairly blaming CIOs for the emergence of variability in identity management processes.

“ *Users lose their trust in the IT department and the CIO.* ”

2.3 Shadow IT

This term refers to **devices, software and services that are not controlled by the IT department** and are therefore not expressly approved by the organization. Basically, we are referring to the situation where a person in the organization decides to use a cloud service without the company’s approval. It is very common for task or project management applications, or organizer applications.

The problem lies in the fact that the company may be exposed to undesired risk, such as the use of data by those applications without the proper protection. This practice is two-pronged; on one hand, it is a threat to security, and on the other, it is an opportunity for people to work with the applications that work best for them.

However, in our case study, Shadow IT poses a threat due to being unconnected to the core directory. This generates more identities without a central management, chaotic processes and security breaches.

Another risk that may result from Shadow IT is **dependency on a provider.**

Major service companies such as Microsoft, Google and Amazon design their infrastructure as large conversion funnels that have the end goal of creating a dependency as providers. Once they have the person’s identity as well as that of the company, they may block service so that you eventually need to pay for them. It is a widespread practice as a customer engagement method. Once they have your identity and you use their services, little by little you will exclude other alternatives and the company will commit to paying for the services.

2.4 Identity breach

Nowadays, our property and assets are more connected than ever. Companies and organizations operating in globalized markets demand agility and efficacy in the workplace.

This connectivity makes systems vulnerable against security threats, and the most common among them in the security of organizations is identity breach. According to the Breach Level Index (BLI), **identity and personal information theft and assumption comprised 53% of all security breaches** for the year 2015.

There has been a change in the modus operandi of digital criminals. Statistics change: identity and personal information theft attacks increase in relation to the theft of credit card numbers. For example, companies such as JPMorgan Chase, MySpace, eBay and Yahoo have suffered identity theft. The largest one recorded by BLI was JPMorgan Chase with 83 million pieces of data breached in 2014.

But identity and information theft are still growing at an alarming rate. The latest Equifax case exceeds 143 million pieces of data of American citizens – about half the country.

3. The Solution

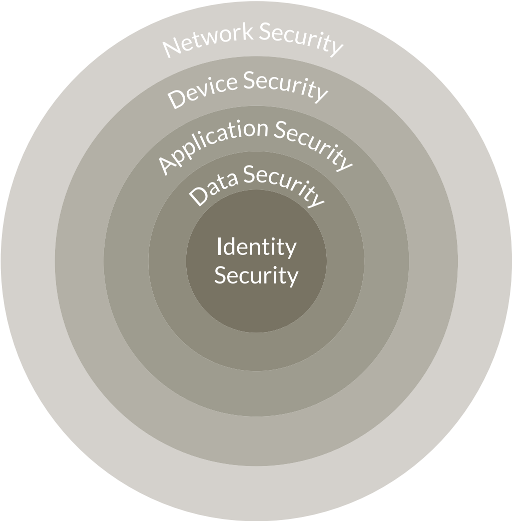
From the outlook of the challenges faced by a CIO, we can then identify two items that must be addressed:

- **Efficacy:** The need to streamline processes and reduce variability
- **Security:** Improve the security of company identities and data

The solution to these problems does not simply depend on installing an antivirus or firewall. These security measures are now obsolete and inadequate to address current risks.

In order for an organization to have a high level of security, five layers should be complied with:

- **Network Security:** mainly composed of firewalls, systems to detect and prevent intrusions (IPS and IDS) and VPNs
- **Device Security:** devices such as servers, computers, notebooks, tablets and mobiles
- **Application Security:** both for internal and web-based applications
- **Data Security:** Data encryption
- **Identity Security:** the core of corporate security



Based on what we have seen as problems and needs, solving variability in system identity, password and access management is the key solution to improve efficacy and security in the company. In other words, we need a system that keeps the variables of each process under control.

It is recommended for this system to have three key features: **integration of all user data, prevention of system variability** (preventing human intervention) and **system flexibility** in order to guarantee changes in processes of the organization.

The IT department should work in conjunction with the company policy, which will be charged with setting forth the granting of access privileges. As a result, all individuals and services will be properly authenticated, authorized and audited.

Integration of certain commonly-used applications in a centralized identity information management solution is a difficult challenge. It requires involving various departments and processes in an organization: from partners or high management, all the way to areas such as customer support.

Good results and benefits can be achieved by implementing an Identity & Access Management (IAM) system with the help of all company actors, their will, and their commitment.

As a result of this solution we will know that employee, provider, partner and client identity management related to internal and shared services and SaaS will be secure and will improve process efficacy.

So now we know **what we need to do,** but we still need to know **how we are going to do it.**

3.1 Identity Access Management (IAM)

The purpose of IAM, which stands for identity access management, is to manage data related to user profiles in one or several applications. It is an interrelated solution that can be used to manage user authentication, account profiles, passwords, rights and access restrictions, as well as other attributes that management of the application may require.

This system is an identity and access manager that integrates policies and organizational processes. Its purpose is to ameliorate our main problem, facilitating and controlling identities and accesses within a company.

These **interrelated solutions** are mainly based on:

01 **Password requirements:** A high-end computer cracks a password in 5.5 hours. Experts recommend for one password requirement to be to contain 12 characters. In order to increase the level and complexity of security the following factors need to be taken into account:

- Password length
- Uppercase and lowercase
- Numbers
- Special characters
- Password reuse time

02 **Multi-Factor Authentication (MFA):** Employees are prone to using the same password across multiple website, which makes them weak and increases the chance of a bad storage. MFA is a complement that improves security in a standard password. For instance, fingerprints and retinal impression.

03 **One-way Hash & Salt:** your identities should be encrypted in a single direction of information transfer. This makes its decryption extremely difficult.

04 **Training:** identities are closely linked to our behavior as users. It is therefore important to raise awareness among employees about the latent dangers of identity theft and assumption.

05 **Use of SaaS identities:** cloud directories such as Google Apps are extremely effective, because they require little investment and IT maintenance. However, they do not offer a directory-level degree of control because these types of Apps were not created as true directories. That is to say, you will be unable to create groups, automations or security layers for logins and identities. This generates more resources to verify each of the applications and services in a business.

In order to accomplish this, it is recommended to implement SSO (single sign-on) via the Identity & access management system, integrating the various cloud applications and local resources in order to provide a solution for modern businesses.

3.2 IAM Usability

As a CIO, you should identify the security and control needs of your organization. In this case, you should choose the various types of authentication bolstering based on the user's usage logic. These are a few common examples:

- When a device is used for the first time
- When a client performs a transaction that he does not usually do
- If a user stays inactive for a long time
- Several actions within a short period of time

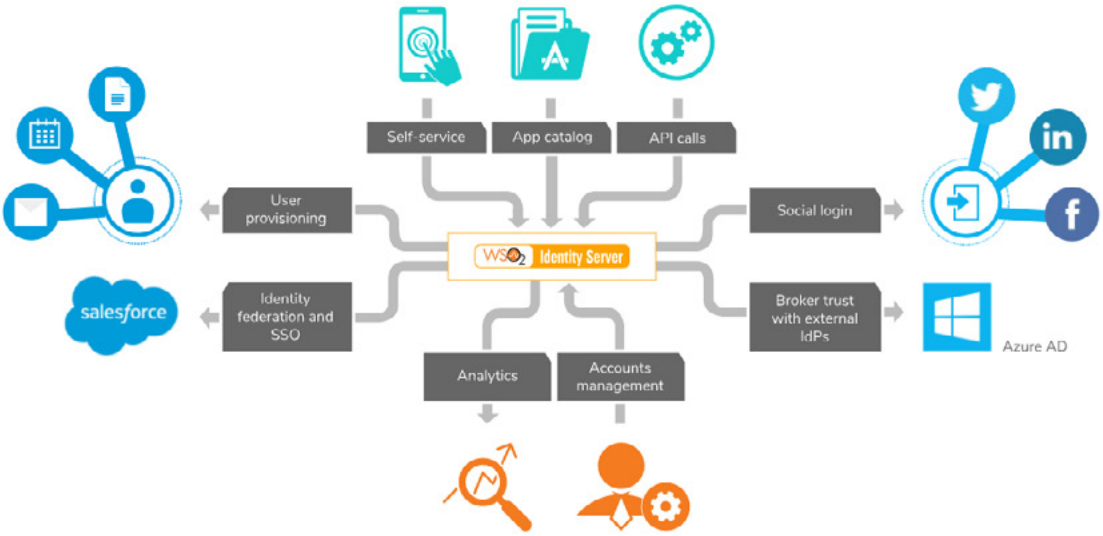
Once they are identified, focus on the best solutions that make the installation and migration work as agile as possible.

> *"Do not plan a mass IAM infrastructure customization. Instead, focus on solutions that allow for a rapid configuration that increases the migration speed..."*
>
> **— Gartner, 2015 —**

There are a number of options out on the market, but we will focus on WSO2's proposal since it offers a comprehensive solution and provides a uniform security service.

3.3 WSO2 Identity Server

WS02 Identity Server is an open-source system based on the strong points of the most widespread security standards. It offers a platform that allows CIOs to apply a uniform layer of security over existing assets in the digital environment. One of its advantages is that the project is in constant evolution, which allows for continuous improvements on each new version. This is of great significance, since it is a system that can face up to new business challenges, customer expectations and cyberattack threats.



Graph SEQ * ARABIC 2: Image via WS02

How does WSO2 Identity Server work?

WS02 Identity Server offers security management for company web applications, services and APIs. This systems allows for a reduction of the time it takes to provide an identity, guarantee secure online interactions and offer a reduced login environment. Other functions include the creation, maintenance and deletion of user accounts across multiple systems, including Cloud applications. This system allows for a **centralized identity as a Service Provider,** a model that guarantees greater efficacy.

End users will get the ‘Jaggery’ interface. In addition, interface login and consent pages may be **fully tailored** to the needs of each organization. The most interesting aspect is that it is run as a web application in an independent context.

{ jaggery.js }

The delicious Javascript framework

Main features

Single sign-on

Capable of establishing bridges between system single sign-on protocols such as OpenID Connext, SAML 2.0 and WS-Federation which offers a unified SSO experience.

Strong and reliable authentication

It is possible to implement multi-factor authentication (MFA) with password on SMS / e-mail (OTP), Fast IDentity Online (FIDO), MePin, Duo Security and more.

Identity governance and administration

Allows for the management of users or user groups with automated workflows. May be implemented as a core element for the governance of identities, facilitating integration with other identity providers such as Google, Facebook, Twitter, Salesforce, among others.

Entitlements and access control

Authorization via role and attribute-based access control through XACML policies. Offers an integral security model based on OAuth 2.0 to ensure access to the APIs.

Monitoring, reporting and auditing

CIOs may analyze authentications and integrated reports as well as audit privileged operations. Allows for a better comprehension of user application authentication patterns. Tools are provided to obtain information required for these analyses in real time and in batch mode.

Integration with systems to enhance capabilities

The system lets you build customized solutions tailored to administration and multi factor authentication requirements by using a wide range of connectors for WSO2 Identity Server.

4. Conclusions

The management of identities and accesses which are part of working processes is a critical aspect for companies. This interrelated management includes all user data, and therefore involves critical, high-variability processes. Mismanagement and a high process variability may result in major setbacks for the company. Moreover, poor management affects employee and company executive perception in regard to the effectiveness of technology departments and the CIO's image in particular.

Companies, and especially CIOs, should be especially careful when applying IAM systems. Using services such as WSO2 Identity Server ensures addressing the two main problems incurred by identity & access management: efficacy and security.

> “ *For every great problem there are always individuals and companies that are looking for solutions to this so-called “identity crisis.* ”

¡Thank you!

About Chakray:

Doing the right things

Chakray, WSO2 Premier Partner, brings together a highly qualified team to offer architectural, consulting and training services for Critical Information Systems. In Chakray we are experts on developing serious and professional Open Source projets with the most innovative WSO2 technology. Our main objective?: To make the best of your company’s technology.

Do you want to improve your systems? Ask our experts.

Ask our consultants without compromise.
We will help you find the best solution for your project.

CONTACT US

CHAKRAY

DOING THE RIGHT THINGS.

WITH THE RIGHT TECHNOLOGY.
TO SUPPORT BUSINESS.

info@chakray.com	www.chakray.com	in	