





### Modern Identity Security Platforms

Where Identity Governance & Administration, Access Management and Privileged Access Management unite to enhance Cybersecurity











#### Agenda

- 1. Executive Summary
- 2. Basic Concepts of Cybersecurity
- 3. Fundamentals of Identity Management
- 4. IGA, AM and PAM
- 5. Identity Security Platform
- 6. Q&A



## Executive Summary

WHAT IS THE PURPOSE OF THE LECTURE



## The purpose of the lecture is to show you what Identity Management as a part of Cybersecurity is and how its tools and platforms enhance cybersecurity

- After the lecture you should know
  - · What are the main objectives of cybersecurity
  - What are the fundamental concepts of Identity Management
  - What is Identity Governance & Administration
  - What is Access Management
  - What is Privileged Access Management
  - How an Identity Security Platform is built and what are its benefits
- With the information from the lecture, you should be able to
  - Protect better your digital identity
  - Contribute to the cybersecurity of your company (and your personal one)
- And hopefully you would like to get more information about the topic and ask specific questions ©
  - · After the lecture
  - At the networking event



# Basic Concepts of Cybersecurity

WHAT DO WE NEED TO PROTECT

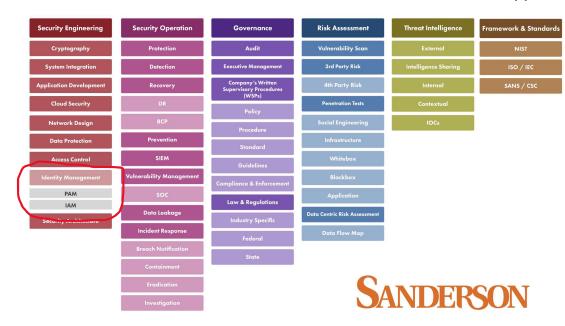


### The Cybersecurity domain is big and topics (and of course specialists) lurk around the corner

- The Cybersecurity domain is divided in 6 main divisions
  - Security Engineering
  - Security Operations
  - Governance
  - · Risk Assessment
  - Threat Intelligence
  - Framework & Standards
- The skills required for each division and its subsets differ widely
  - · System administrators
  - Developers
  - Lawyers
  - Hackers ☺
  - · etc.
- Today we are going to talk about Identity Management
  - No other fields (or at least at absolute minimum)
  - The prerequisites are deliberately set to minimum in order that many people participate and get acquainted with the topic
  - If you still have questions which violate the points above:
    - · Ask them after the lecture
    - Ask them at the networking event









## To be sure we are doing something meaningful to enhance cybersecurity we need to be sure it fulfill its objectives

- Cybersecurity has 3 main objectives
  - We are going to find out soon what are they
- Every measure from all cybersecurity divisions fulfills one or more of these objectives
  - They might be preventive, corrective or detective
  - But they fulfill the same objectives
- Have always that in mind when planning something or wanting some budget

- Чичо, дай пет пари! - каза детето и веднага засрамено си наведе и извъртя главата със захапан пръст.

Гавазинът обясни на консула, че детето иска пет пари.

- Защо ти са пет пари? - попита гавазинът по поръка на консула.

Но детето бе научено само да поиска пари, не бе му казала майката защо му са пари и затова вместо отговор то повтори:

- Чичо, дай пет пари! - и пак се засрами.



#### Physical security and Cybersecurity have some objectives in common

- When you take security measures at home what exactly do you want to achieve
- Primarily you don`t want anything to be stolen
  - You want to have all your possessions
  - This means that they are **available** to you
- The same concept applies with data
  - You want your data to be available to you
  - Access it 24/7 without restrictions
- Availability is the first objective of Cybersecurity





#### Physical security and Cybersecurity have yet another objective in common

- When you take security measures at home what exactly do you want to achieve (although you might not consider that as a security measure in this context)
- You also don`t want to be seen.
  - You need some privacy
  - The things inside the house must remain confidential
- The same concept applies with data
  - · You want your data to be shared only with the people you want
- Confidentiality is the second objective of Cybersecurity





#### The third objective is not associated directly with physical security

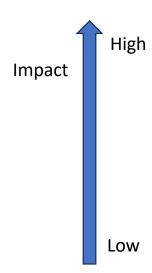
- However, in the past (and to an extent still in the present) it is very popular, especially when we buy expensive goods
- You don`t want to wear adibas or mike
  - You want to possess authentic staff
- The same concept applies with data
  - You want your data to be complete, trustworthy and not being modified or accidentally altered by an authorized user
- Integrity is the third objective of Cybersecurity





#### The consequences of a cyberattacks can be very grave to an enterprise

- These are some examples of what an attacker can cause
- Ransomware
  - In this attack the victim`s personal data is encrypted and unless a ransom is paid won`t be decrypted
  - · All three objectives of cybersecurity have been compromised
    - Availability is compromised since the data is not available to the victim
    - Confidentiality is compromised since most probably the data was copied and made available for sale on darknet
    - Integrity is also compromised as even if we pay ransom and recover the data, we don`t know if it had been modified
- · Denial of Service
  - This attack is designed to force a website, computer, or online service offline. This is accomplished by flooding the target with many requests, consuming its capacity and rendering it unable to respond to legitimate requests.
  - · Here only Availability is compromised

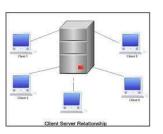




Defending against Cybersecurity attacks is like wrestling permanently in the par terre position

















\$15-16-07 33:41:13:336 TWO (Asset) org. specto history sethings sethings supposed by Leeded properties. Free history-extitions
265-th-f7 (5:45:11,765 DFC [sets] org. spects Auton metrical inpl. detrice(patential); Sciential amounts parted on 18 accord(s).
2013-16-37 20-91-15-399 1990 (solid) org.sepide Anthog.enCrisiz (tigli. Not/Acity) (butter): Suprisis, method: cyclon started
265-16-17 SL-65(1), AM SWE (nota) org. specta Automorphis Sensibility Counting with colony.
2013-10-17 2019013.400 EURO (BUTS) org.apache Folloss Hapred Almedical Winds Hophedock Job., Service: 306_5440062781978_EUIT, 10041. (org.apached
2015-19-17 IS-15:15:16 TWO [Refs] org. specie Autop paped Servicities Steeping for the before netroping agets, that self you.
2010-10-17 31/0112,00 100 [mits] org.spale.nebog.neprel.htm20150 representation.tack.dtr for UNIO. (htm): http://doi.org/10.100
2615-35-27 tit-05:12,712 1976 [main] org specie hadron cost distriparation deprecation; sender, 14 to depresand. Depres, the 67s detrice, sender,
2013-19-17 3119113,000 3990 [eath] org.spathr.Judop.yarv.utvt. Prochabonstrees Prochabonstrees correctly to supported only as \$13.
DRES SELECT SELECTION OF THE PARTY OF A RESERVE AND A SELECT OF THE PARTY OF THE PA
2015-18-37 30/91/14/209 1990 (Heb) org. spacks Jadoop. sapred Saptack: Presenting sptotic hith: //fetra-sa-41/900A/saprapatz. 3x0-40041888-33421778
NLS-19-37 SS-GF-14_392 1999 [sets] org.upache.huloop.raprod.mapfastr (1994/992 e test 2011-05619961594)
2013-10-17 20 40 D1,100 3070 [MILE] org. sporte Audoop. Augrest. Rapheton, Stefs. (p. 1047-10). 189
2015-19-17 251-0514,190 SMH [Instit] org. specia ination_represt mollest: soft Units at 6346000
2015-08-17 (THIS) LEGIS THE (MILE) MG AGAIN ANNING ANGERS RESEARCH SUPLEM V SCHOOLS V SHOWING
posS-se-sh stilles, set shee (seta) org, specte Aeloop represimentatik kontent ik botsetet ik botsete i enote i
2013-10-17 10:00:15,113 1070 [vota] org.specta Judosp sepret Auditor. Fig. setpot col/textor clied a org.specta-belon, sepret Auditor/Settler
per5-sh-sh-sh-sh-sh-sh-sh-sh-sh-sh-sh-sh-sh-
2016-19-17 20-41-17,305 2076 [sets] org.specie Andrey supred Auglicia Seletaria is 6y Indiana - 80271806; Indiana - 80487666
pass-se-IP colors (A) set Twin Twin Train or seach Autocompand restain forces: - solicesectes (See Constitution Constitution - characteristics); heaps - characteristics
2015-15-17 StreEr17,306 1890 [socia] org.apache.Justeup.eapiref.Aapfashr. [EQUATED] \$1209776 Not. \$4216940[\$7120718]
DELS-18-17 TECHS IN DOS INFO (SELLETORAS) org. southe hadron magnet markets visitated spill to
2015-19-17 at mile job 1970 [sate] org specte hadron caprost hadron (19818) equator \$710076 by address(1980906) but attended (1980) organization (1980).
DREST SECTION OF THE DESTRICT OF THE PARTY OF SECTION OF THE PARTY OF THE DREST OF
2015-18-17 (Cold-Digital SING (Salis) ang apaste Joseph Aspend Aspend Salishin Substant a 1738070; beford a 160070; beford a 20007000
propries of the contraction of t
2015-10-17 IS-05-18-00 1070 [sets] org. spacks Andreas Anglesia: (EDOATOR) SALURIA Set. 20120-00(001170)
pota-se-or micro-cours sere (ppt//mneed) org.aquota.haboo.haprod.mprasic victorad spill o
2015-10-17 IS-IN-18-(23 1000 [satu] org. specie-bashup supred Saffanir [10120] reputer \$01201 in 201500(101120) lot, \$1000(20100)
2013-18-37 33140.40,307 3070 (NITA) org. specie Antice andred metals gold to income
2015-18-17 31-15-15-16-167-1870 [arts] ang apada-bahang-majoral Replindo Substant a SASSISSE, Mobile a SASSISSE, Aufordo a SAS
productional production (settle) orgularity has produced and production and production of the producti
2013-16-17 IE-IE-IE-JUST 1870 [nets] org-specie Audiosp.coprod. Repliesio: [1904/00] 47684603 tot: [4776001(97164014)



## In almost all cases however the attacker gains access to the system with existing (compromised) account

- This is why Identity Management is so important!
- With the components of an Identity Security Platform, we are minimizing the risk of this event occurring
- You will see later how



## Fundamentals of Identity Management

Let's get familiar with some terms before we see the real thing



#### We start with the first two tangible concepts user and target system

• The first two core elements are user and application



- User
  - This is the real physical person trying to gain access to a target system (application)
  - In some cases, however the user might not be a physical person
    - A printer has also a user
    - Back-Up Software has also some users
- Target System
  - In the language of Identity Management any application the user is trying to get access is called target system



Target system



#### In order to access a target system, the user needs an account and corresponding credentials

 The account and the corresponding credentials are the means to get access



User

- Account
  - · Accounts reference a set of permissions and privileges needed for an application or asset to connect or operate
- Credential
  - A credential is an account with an associated password, passcode, certificate, or othertypes of key.
  - · Credentials can have more than one security mechanism assigned to them -this is called dual or multifactor authentication





Account-Credential



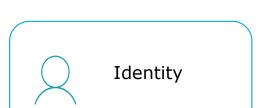
Target system



User

## The multiple accounts and assets one user possesses are aggregated into an Identity

- Every user has only one Identity
  - Some exceptions are possible e.g. when a doctor becomes a patient in the hospital, he/she works
- It contains all accounts and assets of a user
  - Imagine the car key and the house key in your pocket
- However, two big questions remain open
  - · How can do we get information about the user in the system
  - · What access rights do we have in the target system





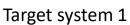






Account-Credential 1 ••• Account-Credential n





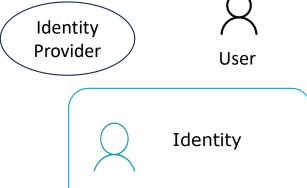


Target system n



We need an Identity Provider (IdP) to provide us with information about the user

- Typically, in an enterprise, the HR system is the primary identity provider
  - It gives us the information about the employees (their type/department and other information relevant for their access rights)
- For external users, external IdPs are used
  - Strong IdPs such as Bank ID or National ID
  - Weak IdPs such as Google mail or Facebook
- Typically, a secondary identity provider exists in an enterprise in the form of directory (most common Active Directory (AD))
  - Applications get the login information from AD (there the accounts and credentials are typically stored)
  - However, the AD must get the information from somewhere (its first use is as a target system)
  - Of course, you can let HR create users directly in AD very bad practice









Account-Credential 1 ••• Account-Credential n





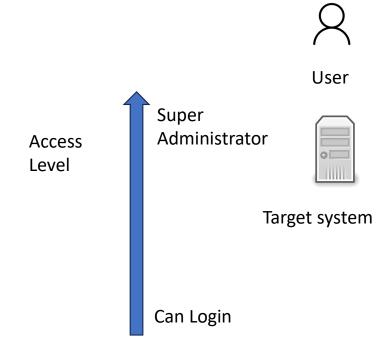
Target system 1

Target system n



#### We need to determine what form of access we have for each target system

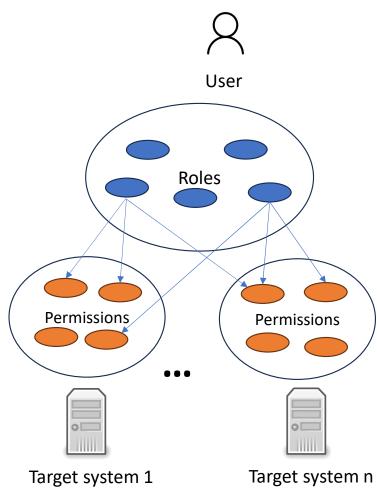
- The granularity of access can be very complex
- For every little element of the application/asset following combinations could exist
  - Create the user is allowed to create a new element
  - Read the user is allowed to read the element
  - Update the user is allowed to update the element
  - Delete the user is allowed to delete the element
- · Additionally, some functions could be usable/not usable
- There are also some rules to be followed
  - Least Privilege give user the least possible privilege (access rights) to do the job
  - Need to know provide the user only with the information they need to do their job





#### Using roles, we can define user access very granularly

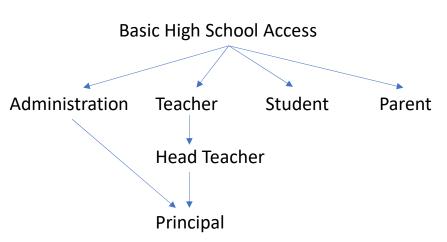
- One Role contains a subset of permissions
- One user or more precisely said his identity can have multiple roles
- · Most target systems have already roles defined
- · So we need just to assign the roles to the identity
- The permissions specified in the role are called **entitlements**





## Modelling and assigning roles is very important and has some aspects to be considered –Hierarchy and Separation of duties

- · Roles have a hierarchical structure
- Every role has the entitlements of the previous one plus extra ones, e.g., a Head Teacher has all entitlements of a Teacher
- However, certain roles cannot be taken by one user at a time
  - Can a Student be a Teacher?
  - Can a Principal be a Parent?
- Sometimes the answer it depends and then:
  - **Compliance policies** determine if having the roles is forbidden or not
  - Compliance policies can and do change all the time
  - Thus, a violation can occur where there was none





## IGA, AM and PAM

The three pillars of Identity Security



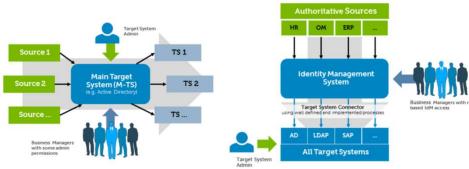
## Identity Governance and Administration

The central place for governing Identities



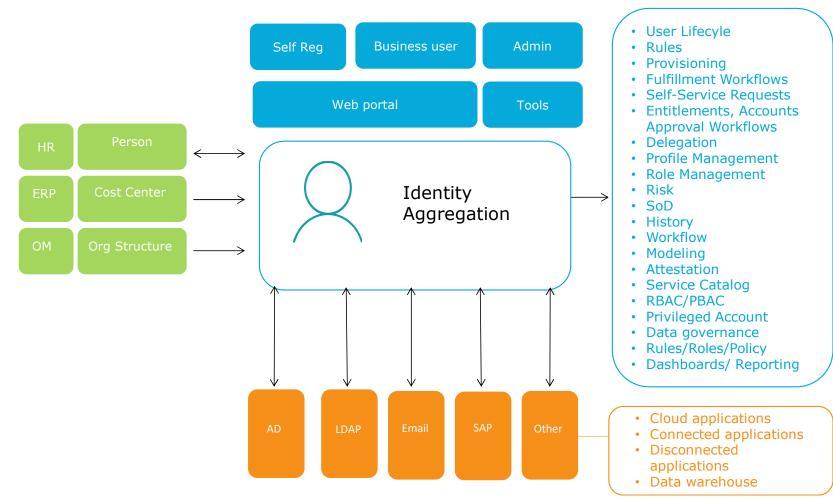
## The old world before Identity Management was Target-System Centric, opposed to modern IDM centric approach

- In the old world
  - Target System Administrators gave directly rights in the target system
    - Not knowing exactly what to give as entitlements
    - Perfect way to violate confidentiality as accounts are overprivileged
- In the new world
  - The information about the user comes directly from the authoritative systems
  - Business Managers can give additional access if requested but everything is tracked
  - · Compliance policies in place to detect and prevent violation



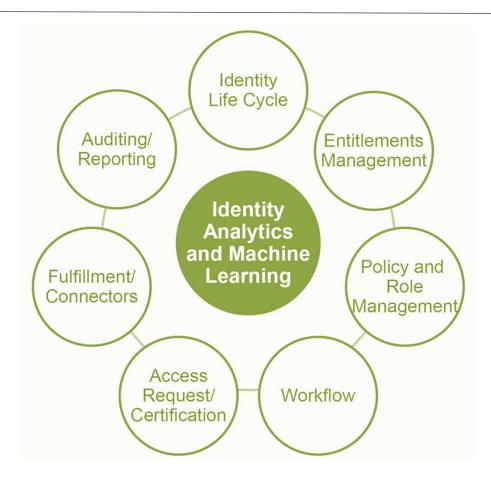
## The Identity Manager aggregates the information about the identity and enables all functions for Identity Governance & Administration





#### The IGA has 7 core components

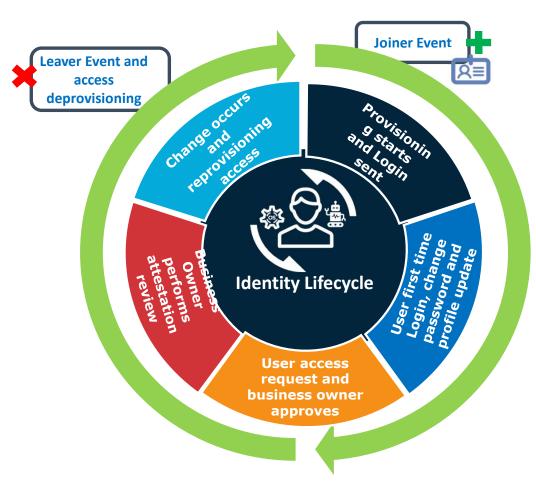




## Identity Life Cycle Management makes sure we cover all type of users during their tenure at the company



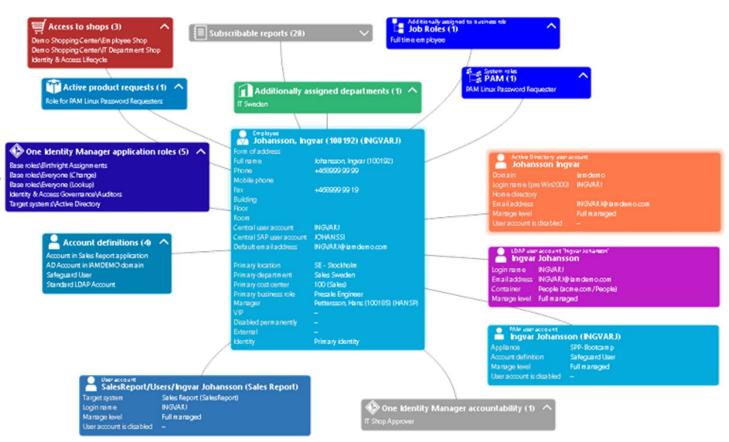
- Employees
- Contractors
- Customers
- Nonhumans
  - (RPA bots, service accounts)
- Manage joiners, movers and leavers
- Support for delegation
- Self registration



## Entitlements Management maintains the link between Identities and Access Rights



- Discovery
- Maintains the link between Identities and access rights
- Entitlement Catalogue
   Base rolect/Everyone (Crarged
   Base rolect/Everyone (Localus)
   Identity & Access Governance)
   Target system s/Active Director

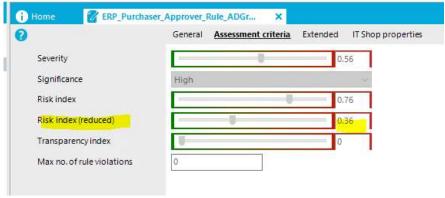


#### Policy and Role Management – we want to ensure that we stay compliant ©



alders, Ans (ANS.AALDERS) - ERP\_Purchaser\_Approver\_Rule\_ADGroups obie, Anthia (ANTHIA.ABBIE) - ERP\_Purchaser\_Approver\_Rule\_ADGroup

- Validity periods for nonemployees
- Grouping entitlements to form roles
- Enforcing segregation of duty (SoD)
- Connection between business to technical roles

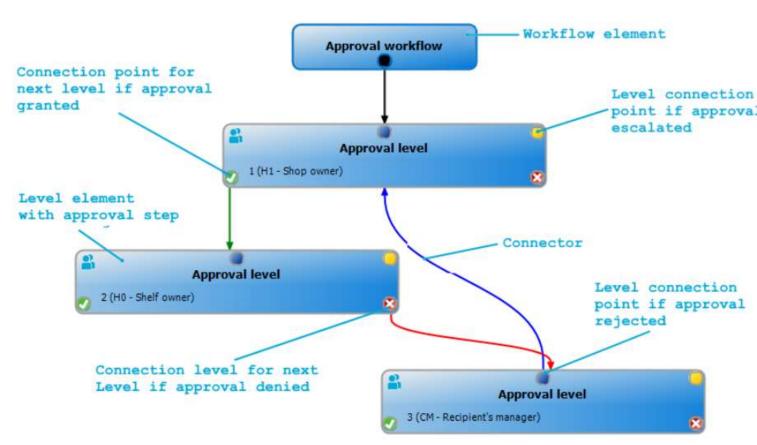




#### For some entitlements multiple approvals are needed – we call this workflow



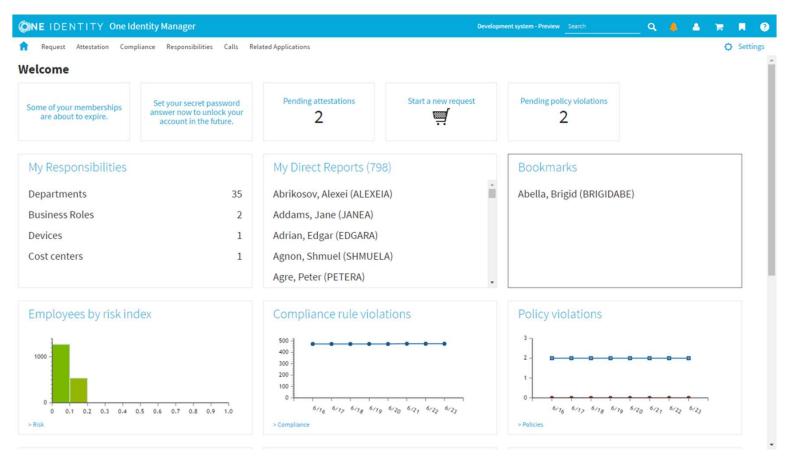
- Workflows with approval steps
- Delegation and escalations
- Segregation of Duties (SoD)
- Support for electronic signatures



#### The User can order entitlements himself



- Self Service
- Request on behalf
- Campaign management
- Certify role composition and entitlements



#### In the enterprises there are a lof of target systems- so we need connectors



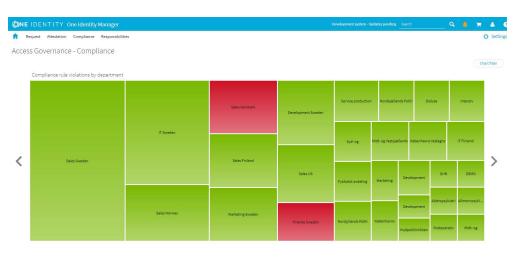
- Direct provisioning with vendor provided connectors
- Service Desk fulfillment (manual)

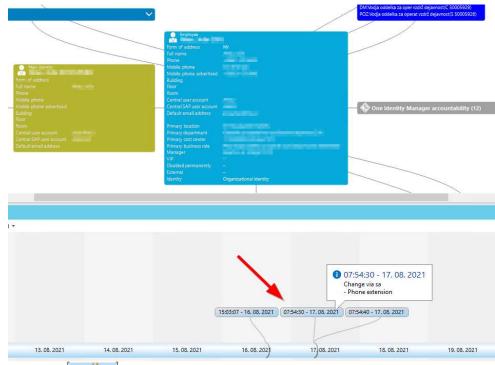


#### Compliance makes us secure and saves money ©



- Policy based controls and monitoring
- Segregation of Duties (SoD) violations
- Object Life-cycle changes







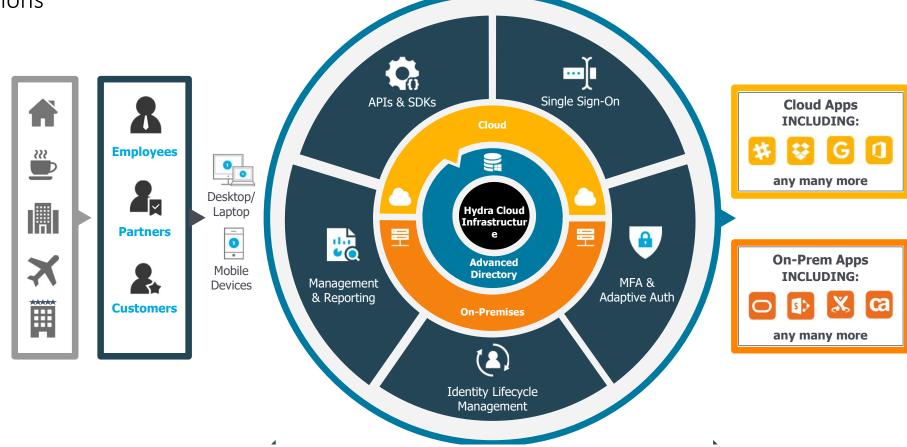
## Access Management

Secure your Access



Access Management is the process of authorizing, auditing and authenticating access

to applications



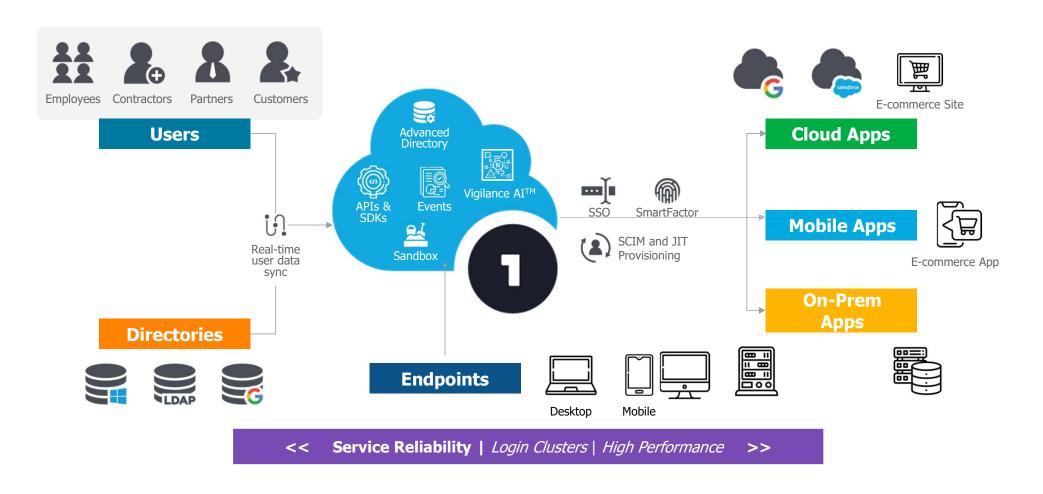


#### Why do we need Access Management





### How does an Access Management Solution work



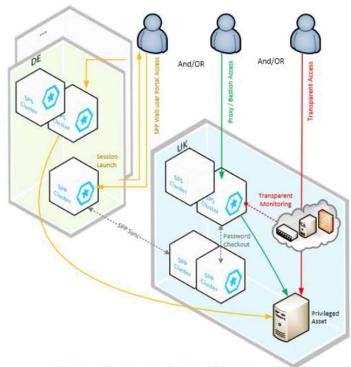


## Privileged Access Management

Secure your Privileged Accounts



The purpose of Privileged Access Management is to have an intermediate session where users can request admin sessions to assets



SPS cluster, SPP cluster

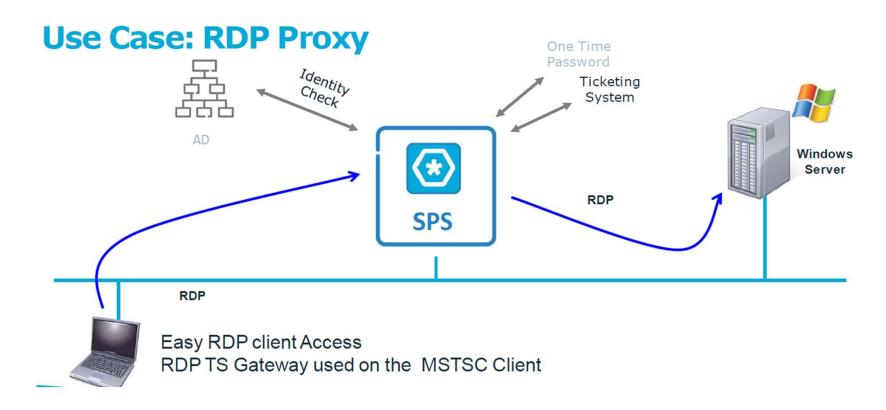


### Privileged Access Management blocks unwanted access





To get a session, the PAM solution checks the identity and gives one time password if the request is approved



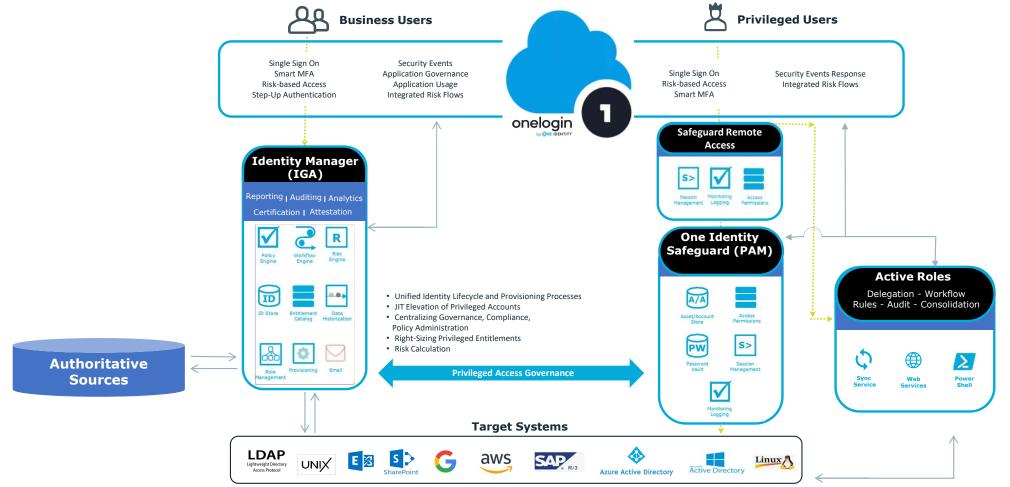


# Identity Security Platform

How do they work together

## This is a sample workflow of IGA, AM and PAM working together based on the One Identity Security Platform







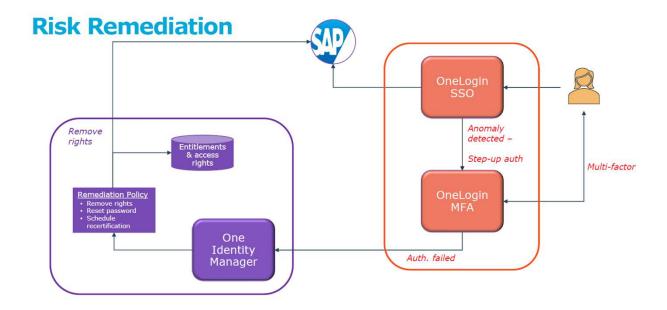
Now we are going to see some use cases how the platform gives benefit

• Hint: Gives security and saves money ©



#### Use Case 1: Deprovision entitlements from compromised accounts

• The combination between AM and IGA can fast remove rights from a compromised account





### Use Case 2 : Enforce Least Privileged Principle

- Entitlements which are not used are obviously not needed ©
- Good input for recertification  $\ensuremath{\mbox{\@omega}}$



### Use Case 3 : Save money removing unused licences

- In some cases, there are a lot of licenses which are not used
- These entitlements can be removed and the licenses cancelled
- Money saved ☺



### Thank you very much for your attention



Ivan Pepelov CEO

IDVKM OOD Cherni Vrah 51 BG-1407 Sofia Mobile +359 896 177 459

ivan.pepelov@idvkm.com