DigitalAlliances
continue collaboration

CISO Alliances

SOUTH AFRICA CHAPTER

17th of February 2022

Results

SailPoint

CISO Alliances

ALLIANCE Media Group

Alliance - 'A union formed for mutual benefit'

CISO Alliances

ALLIANCE Media Group

DigitalAlliances
continue collaboration

Executive Business Exchange

DPO Alliances

CIO Alliances

CISO Alliances

CXO Alliances

CMO Alliances

CDO Alliances

Foreword

Leigh Thomas is an ambitious and passionate executive with a desire for achieving the ideal.

With experience in numerous industries and working within C-level communities across the globe in Oil & Gas, Mining, Power & Enterprise IT, across multiple divisions across the business.

Following his experience with his previous employer and working with leading CIOs & CISO's across EMEA, his understanding of B2B events grew. With his passion for achieving the ideal scenario a plan was founded to strip back what the industry is about. This is where the core values of the Alliance Chapter were born along with Alliance Media Group.
Alliance - 'A union formed for mutual benefit'.

Whilst understanding that every business will need to drive commercials to become sustainable in the modern world. Leigh believed that commercials must not be the driver but, a solution to a 'why'.
The Event Managed Services industry is spiralling into a dark tunnel of an industry where money is the leader and not the value of time. The industry was born off the back of 'Everybody wants to learn' and Leigh Thomas has created the Alliances to ensure that the end user driven meets, are purely focused around the educational needs of everyone involved and around their business objectives. Zoning in on the best practices in overcoming the common business objectives that motivate activity within each of the end user firms and not simply global trends and themes to generate revenue.

2020 and the Digital environment has been forced for a remote workforce with limited human interaction due to the Coronavirus pandemic since March 2020. From this, our community representative have been relied upon even more for business enablement.

From the event space environment, even more events companies have found an overnight solution of plaguing diaries with event upon event, with revenue driven activities. As an organisation, we will shy away from this and only invite the community to engage when justified. We will also, not be looking for time commitments of more than an hour or two as we understand that life is continued, in the remote style of operating business currently.

Leigh Thomas
Director & Founder

12.45

Welcome Remarks & Joining Time

13.05

Focused Session

Session Leaders:

Hans-Robert Vermeulen, Identity Strategist Growth Markets (EMEA) – SailPoint
Michael Steyn, Lead Information Security Officer (SA) – Old Mutual

Session Title:

"Identity Security: From Zero Trust to Total Confidence – Tackling the Identity Journey Step by Step"

13.45

Debate and Questions

14.25

Action Areas and Next Steps

CISO Alliances
DigitalAlliances
continue collaboration

"Identity Security: From Zero Trust to Total Confidence - Tackling the Identity Journey Step by Step"

South Africa

Thursday 17th of February 13.00-14.30 (SAST)
www.alliances.global
Leigh@alliances.global

Hans-Robert Vermeulen
Identity Strategist
Growth Markets (EMEA)
SailPoint

Michael Steyn
Lead Information
Security Officer (SA)
Old Mutual

In partnership with SailPoint

Overview and Supporting Resources

Date: Thursday, 17th of February 2022

Time: 13.00 pm – 14.30 pm (SAST)

Platform: Digital Alliances

Location: Digital Alliances – Microsoft Teams Link – Invite Only

Overall Theme:

Identity Security: From Zero Trust to Total Confidence – Tackling the Identity Journey Step by Step

Old Mutual and SailPoint will take you on a journey through the Identity landscape, discussing everything from the most important first steps all the way to the most mature implementations, as well as the next challenges that CISO's needs to focus on.

Supportive Links:

SailPoint Corporate Overview

Building a business case for Identity Governance

Focused Session

Session Leaders

Hans-Robert Vermeulen, Identity Strategist Growth Markets (EMEA)
SailPoint
Michael Steyn, Lead Information Security Officer (SA)
Old Mutual

Identity Security: From Zero Trust to Total Confidence – Tackling the Identity Journey Step by Step

Old Mutual and SailPoint will take you on a journey through the Identity landscape, discussing everything from the most important first steps all the way to the most mature implementations, as well as the next challenges that CISO's needs to focus on.

Companies have invested in solutions to automate access assignment. Although this often covers only basic provisioning, they feel well protected. This is a false sense of security. Enforcing a least privileged access model is not achieved by "fire and forget" provisioning or account creation. Least privileged stands no chance if we do not see and review changes being made inside applications; if we do not incorporate new access rights and new applications into our existing role model; and increasingly important if we have no clue if access is being used, or if we think that SSO is the answer to our problems.

Takeaways

We aim for everyone in this session to walk away with ideas, plans of action and answers to the below topics:

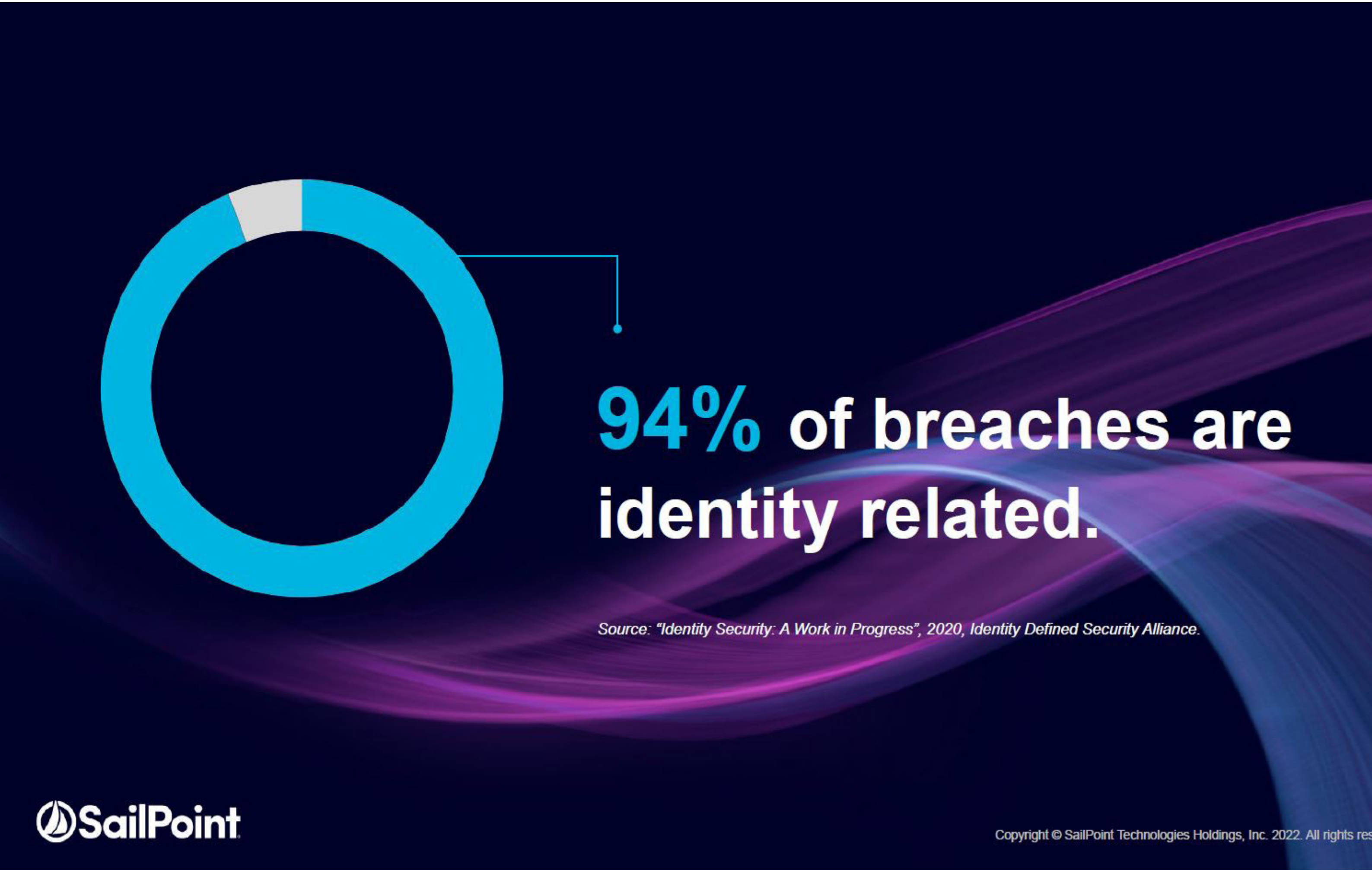
– Starting simple is more important than you think. There is more business value in a simple foundation than many realize

– Why Automated Provisioning can provide a false sense of security

– Artificial Intelligence allows you to take control in complex situations

In this session SailPoint will be joined by Michael Steyn, the Lead Information Security Officer (SA) at Old Mutual. Old Mutual has successfully implemented Identity Security at record pace inside their company. We invite you to actively participate and learn from the experiences amongst the audience, during this highly interactive session where each topic will be introduced for 5 minutes and then discussed for 10.

SailPoint



94% of breaches are identity related.

Source: "Identity Security: A Work in Progress", 2020, Identity Defined Security Alliance.

SailPoint

Identity Defined Security Alliance (IDSA) report stated that 94% of breaches organizations are experiencing are identity related – which shows how prevalent this issue really is

So we have to rethink Identity Security

Moving from Technology-centric to people centric

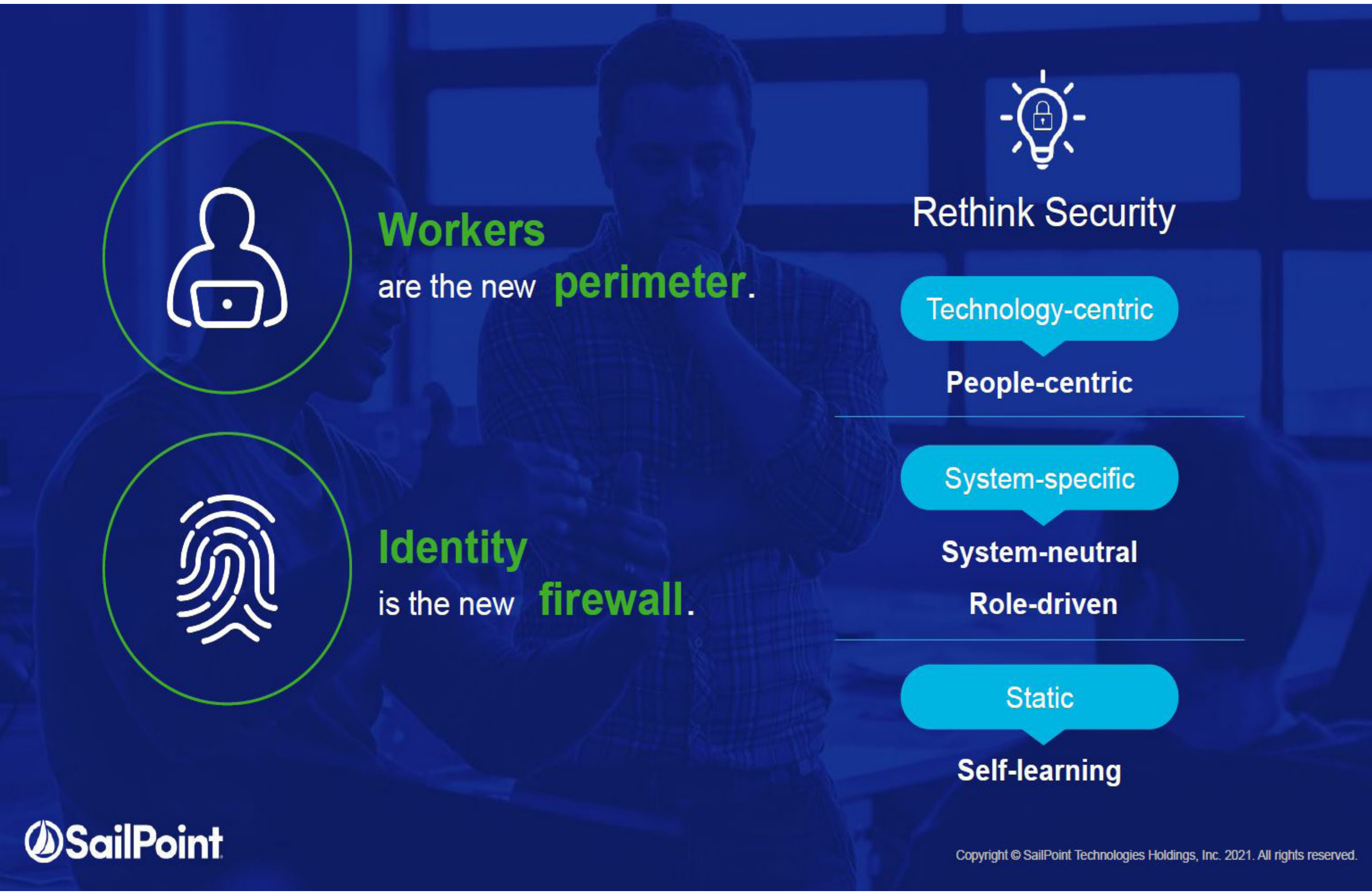
From System specific to system neutral and role driven with more policy at the helm

From static to self-learning by embracing the power of Artificial Intelligence

We have to accept that no matter how many additional layers of security we put into our environments.

Workers are the new perimeter and Identity is the new firewall

A compromised identity typically has way too many access rights, which makes it an unnecessary large attack surface, with an increased risk of actual damage to the company.



Workers are the new **perimeter.**

Identity is the new **firewall.**

Rethink Security

Technology-centric

People-centric

System-specific

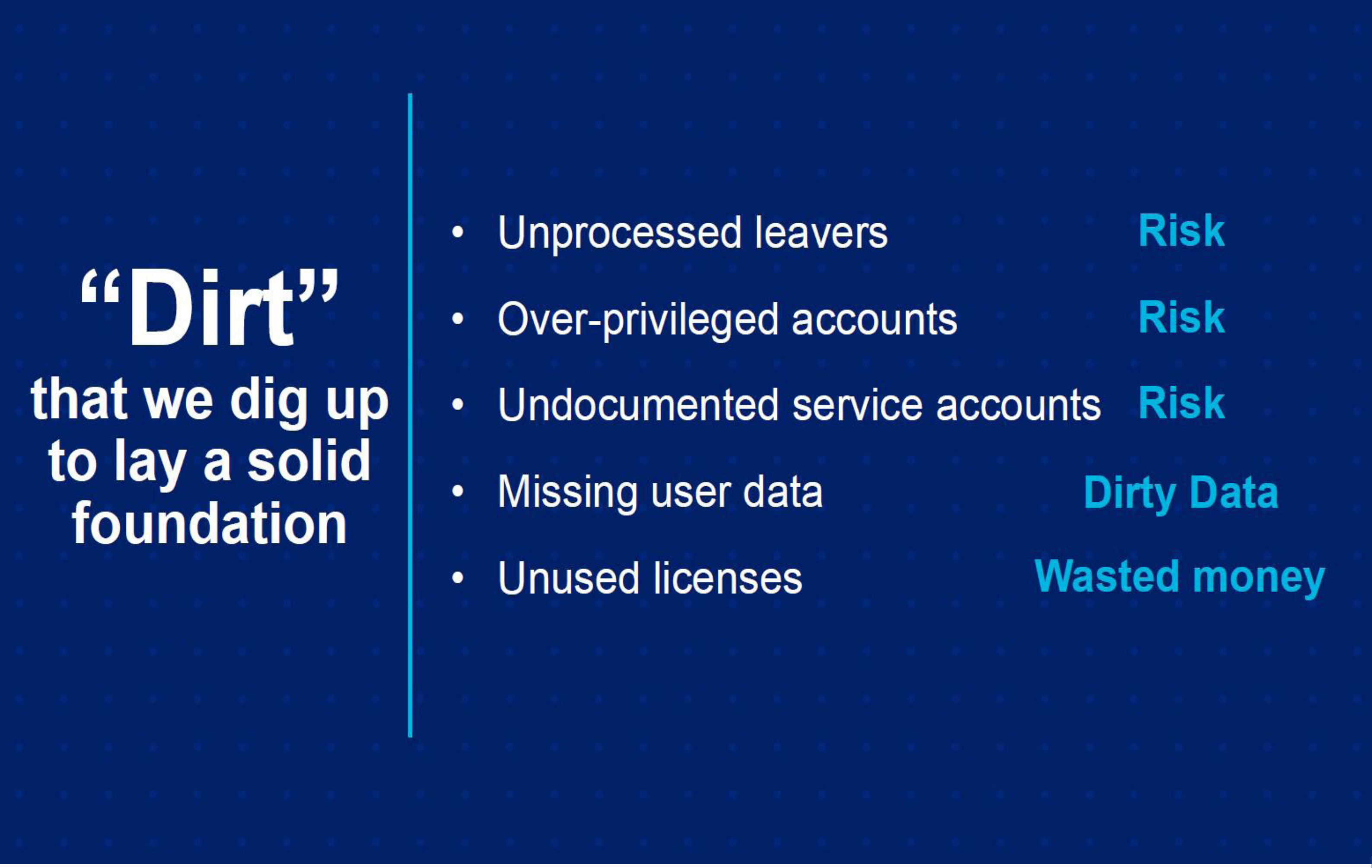
System-neutral

Role-driven

Static

Self-learning

SailPoint



“Dirt” that we dig up to lay a solid foundation

• Unprocessed leavers	Risk
• Over-privileged accounts	Risk
• Undocumented service accounts	Risk
• Missing user data	Dirty Data
• Unused licenses	Wasted money

Just like laying a foundation for a house.
We also dig up dirt. Digital dirt....
But it is that dirt where our first business value is actually achieved.

- Unprocessed leavers
- Over-privileged accounts
- Undocumented service accounts
- Missing user data
- Unused licenses

All of this falls into the category of risk and waisted money.

But it is very important to acknowledge that just by connecting to your systems, we are able to tackle all of these elements straight off the bat. And this level of risk reduction is already critical for all companies as it exposes the flaws in the current process, the mistakes that have been made over the past years and the actual risk that has been sitting in the systems as a result.

Provisioning cannot be a fire and forget one-time affair.

That may be great to set up initial accounts and speed up the on-boarding process, but it does not answer the most basic question of all.

Fire and Forget Provisioning does not provide any protection

“Who has access to what”
How much visibility do you have today?
SailPoint
Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved.

Just think about where you stand.

What really is your level of visibility?

It is a fact that today, the majority of companies are actually struggling massively to stay ahead of the curve, struggle keeping their Risk low and dealing with the ever changing IT landscape.
Especially in today's world of working from home and the insane adoption of SaaS applications.

Some of you may already have invested in an Identity Security or governance program, but even if you have done so, we have to acknowledge that our IT environment is far from static and as a result, we all have to deal with.

- More applications needing to be onboarded
- More governance requirements
- More access rights to certify
- More access requests and approvals to deal with
- More roles to create
- More roles to maintain
- The list goes on and on.....

And because things are ever changing, before we know it, you are almost back to where you started from.

Back to a lot of manual decisions, many individual line items to certify and thousands if not hundreds of thousands of entitlements to manage.

Unless you can maintain it all.

Certification Fatigue

Too much to certify, too little time

Bulk Approval

Little to no context of appropriateness of request

Low Revocation Rates

Access items are no longer relevant to user function

Over Entitlement of Users

Access need is obsolete

Outdated Roles

Roles are brittle and lacking relevant contents

Effectiveness

Having to perform a lot of individual decisions has a negative impact on your governance program.

If people need to make too many decisions, they try and get as efficient as they can and unfortunately, that often means clicking without looking.

- Or bulk approvals.... Select all and hit approve. Because I either don't understand what I am looking at, or I don't have time to deal with this....
- And all of that results in low revocation rates....
- Which means that we are again looking at an unnecessary large attack surface, because people have too much access.
- On top of that, our roles are in need of constant maintenance because we on-board new applications and new access rights get created all the time and if we fail to maintain our roles. Then we are back to delaying with a lot of individual entitlements that need to be requested, reviewed, etc.
- So it looks like over time, the effectiveness of our Governance Program may actually decrease.

Not having a governance program today puts you at even greater risk, I hope that is clear. But I also hope it is clear that Identity Security is not just a project, it is a program, it is a vital part of your Zero Trust strategy.

Knowing this, the conclusion can be that many deployments are in need of constant improvements.

Food for thought

1100 applications? Did I hear right?

Yes, Michael refers to 1100 applications. However the definition of application is important. In Old Mutual's implementation, SailPoint sees each modules within a suite as an applications. For example, the Oracle EBS suite consists of multiple modules and each module is onboarded as an application. Many may see this as one application, however in the Old Mutual environment it is seen and counted as multiple applications.

How do organisations deal with CIAM where you have many customers/vendors etc.. and having to manage the IAM lifecycle? Assume you have many partners/customers, some very small and how do you deal with federation and delegated admin for lifestyle management specifically for leavers?

Most customers separate CIAM from their corporate IGA program. There are many reasons for this, but mostly CIAM is straight forward and they do not require access governance capabilities and typically only touch few systems.

Across the onboarded BU's and mapping back to Employee/HR Master Data (Job Roles), is each of the 1,100 Applications maintaining a separate "Security Level Group" (e.g View Only, Editor, Admin), which could imply that you are mapping 1,100 x 3 = 3,300 Total Security Groups within SailPoint IDN?

SailPoint reads all access rights from an application and adds it to its entitlement catalogue. This is an automated process, so no need to map access manually in order to get visibility or request access. On top of that, SailPoint can leverage a role model to make logical groupings of entitlements of access easier to manage in access reviews (single decision) access request (single request / approval) or automated provisioning (single role for a job function for example). Old Mutual has over 450.000 entitlements in the SailPoint catalogue.

How do you deal with legacy applications with regard to integration

All applications have similar governance requirements, no matter how or where they are hosted. There are a number of "connectors" that enable integration into SailPoint. SailPoint leverages auto-managed Virtual Appliances that run the connectivity platform and allow simple connection to both on-prem as well as cloud resources. Virtual Appliances call home over port 443 and use dual-layer encryption for security purposes. More information about the virtual appliances and the security model can be found at https://www.sailpoint.com/identity-library/delivering-innovative-cloud-security/

Has the tool got the capability to manage local admin rights for user workstations (i.e. granting/removing/reporting)?

There is an out of the box connector to manage "Windows Local" accounts, however it is targeted towards Windows Server 2012 through to 2019.

Food for thought

I have a huge problem with how security teams measure success of LAM programmes. Security teams love to count number of apps integrated, birth rights, access requests, access reviews, etc. No doubt implementing such a technology improves considerably on whatever system / process was there before. Is that enough? In my view absolutely not. Most IAM programmes are funded on the back of audit findings, and as such audits opinion of the risk is a critical measure of success. To resolve audit findings sustainably, you have to go after quality, not quantity. You need to fully resolve uncorrelated accounts, you need 100% response rates on reviews, etc. This is the audit methodology, they pick a sample and look for exceptions. If you are achieving a response rate on a access review of 80% which is great, unfortunately audit don't have to look far to find exceptions. The regulators view of risk is also largely informed by audits opinion of the risk overall. Hope this makes sense. This explains why most identity governance programs globally are struggling. The point here is that technology is only part of the IAM problem, the processes to entrench this in a large organisation are just as important and is often neglected. This is seen as a security owned problem which it isn't. I am not talking about board support which is implied, I am talking about leadership buy in across the organisation. We have to start driving & landing Business Efficiencies. I want to flip this Program into paving an ISO Certification.

- There have still been great achievements in many programs, but it does requires a little "marketing" to explain it properly to senior leadership.

- There have been significant risk reductions, including fraud and breach risks, with very real results in terms of risk reduction and cost savings as a result of the work that has been put into the programs. SailPoint makes it very easy for an auditors to find the anomalies that exist as they don't have to start from scratch and look at samples of the IT landscape, they have access to the entire IT landscape. Once Identity Security is embedded, the auditors are largely ignoring the pieces that are touched by the Identity Security program, all they have to do is focus on the exceptions.

  - What manager did not complete a review? Let's look at their team.

  - What SOD violation was allowed for a period of time (for a valid reason)? Let's look if those access rights were abused during that time.

  - What critical application has not been on-boarded? Let's look there to search for anomalies.

Food for thought

Also agree getting management to take reviews seriously is big issue and is a major stumbling block to making this an effective control.
Does Sailpoint have the ability to identify Segregation of duties conflicts bring this to the line manager to understand what he is accepting in terms of the risk?

Yes, SailPoint offers Separation of Duties functionality in several offerings. From deep integration with your ERP environment, for example replacing SAP GRC Access Controls, to cross application SOD, all is covered by SailPoint.

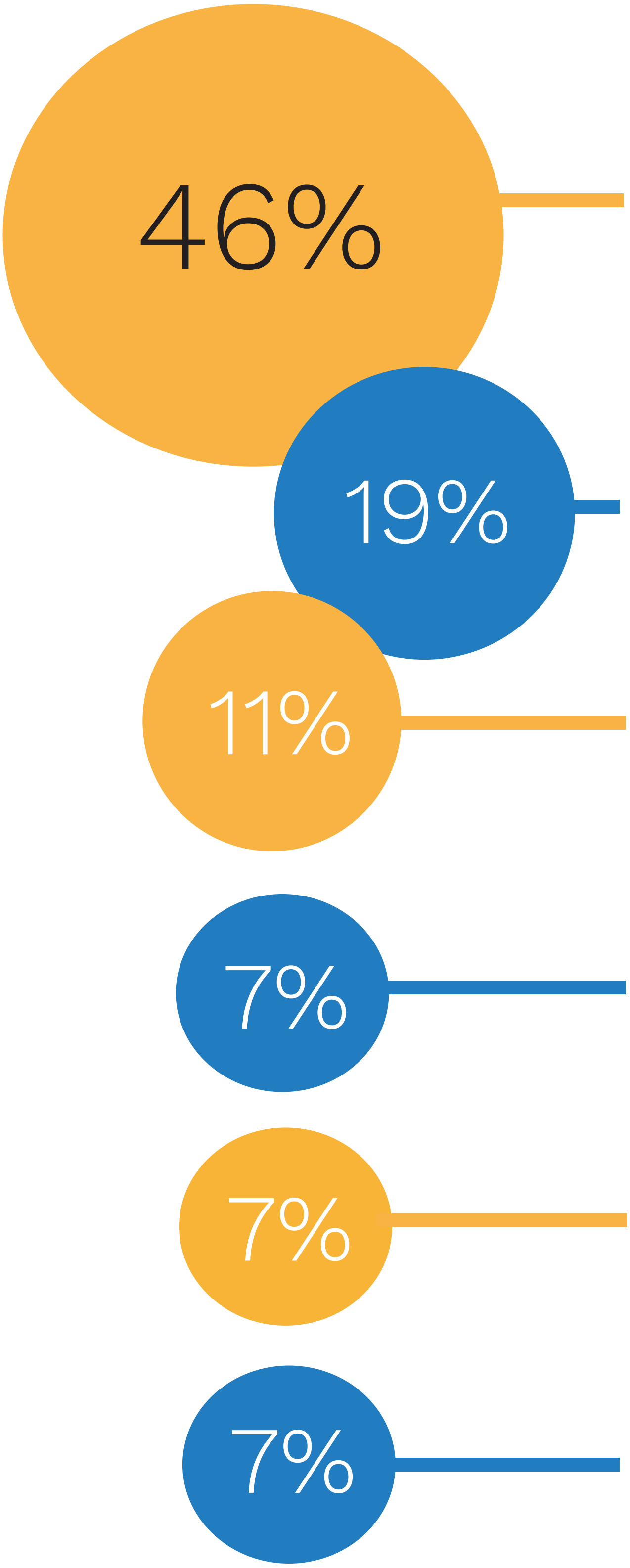
SailPoint

CISO Alliances

DigitalAlliances
continue collaboration

Results

What would you like to see as a next topic for a next chapter from the below?



Cloud Access Management
Getting a grip on the access your people have in your cloud platforms

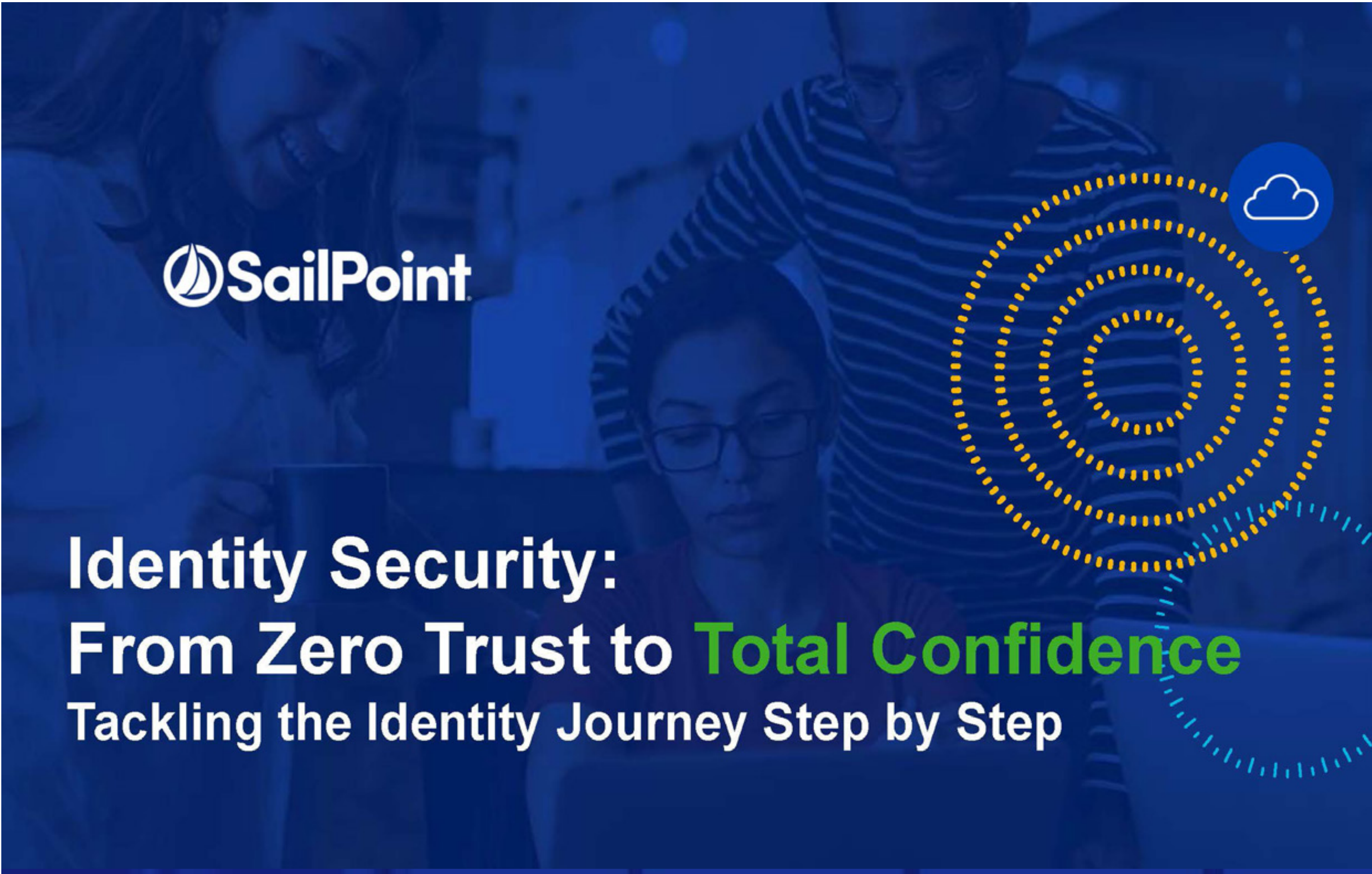
Deep dive into Role mining and business benefits

Deep dive into File Access Management and how it helps to address the right to be forgotten challenge (assuming that is relevant to POPI just like it is for GDPR)

Facing yet another forced SAP GRC Access Controls migration? SailPoint Access Risk Management for SAP – A GRC Access Controls replacement

Deep dive into Access Certifications and its business benefits

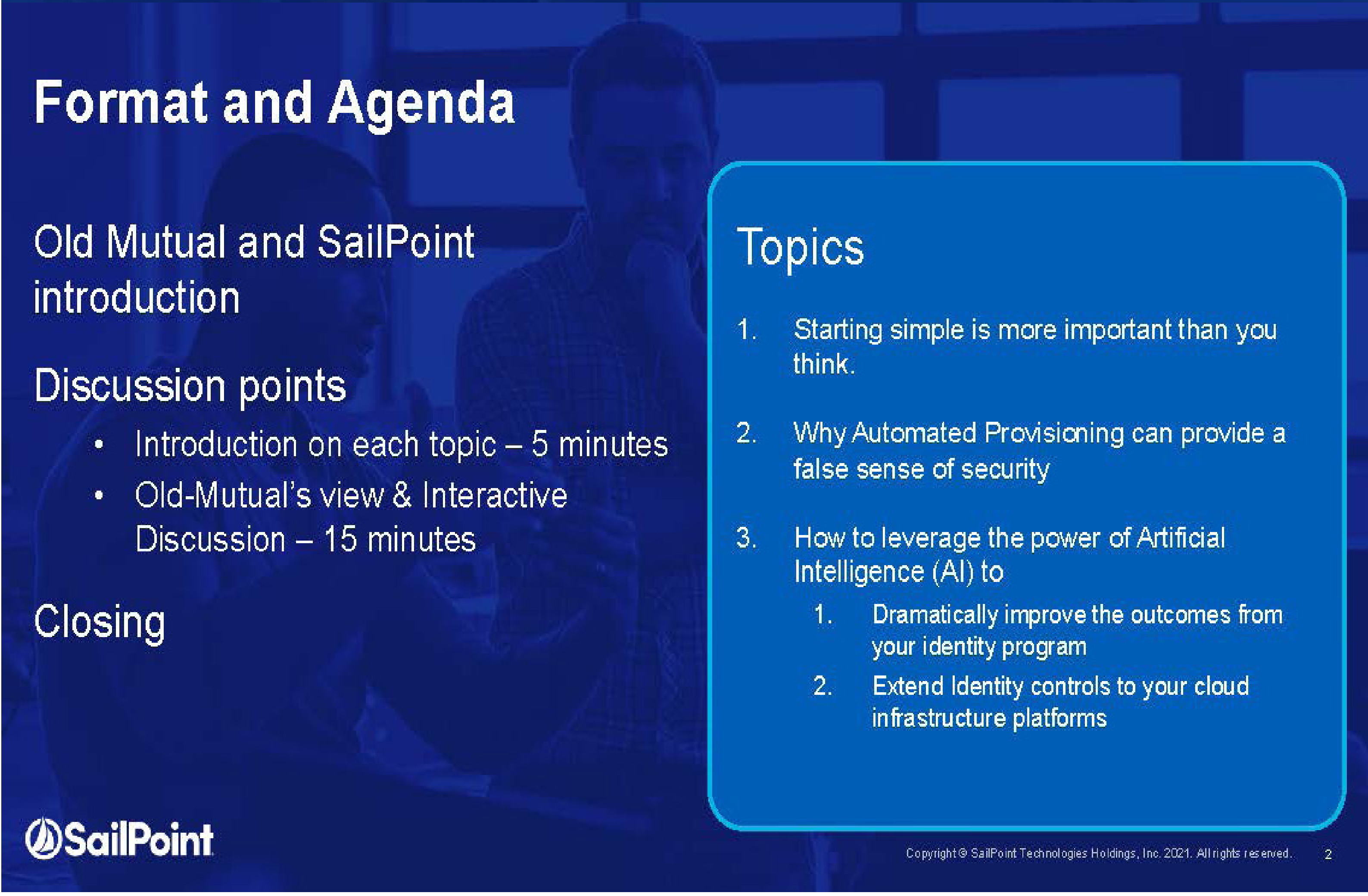
Other - Email to leigh@alliances.global



SailPoint

Identity Security:
From Zero Trust to Total Confidence

Tackling the Identity Journey Step by Step



Format and Agenda

Old Mutual and SailPoint introduction

Discussion points

- Introduction on each topic – 5 minutes
- Old-Mutual's view & Interactive Discussion – 15 minutes

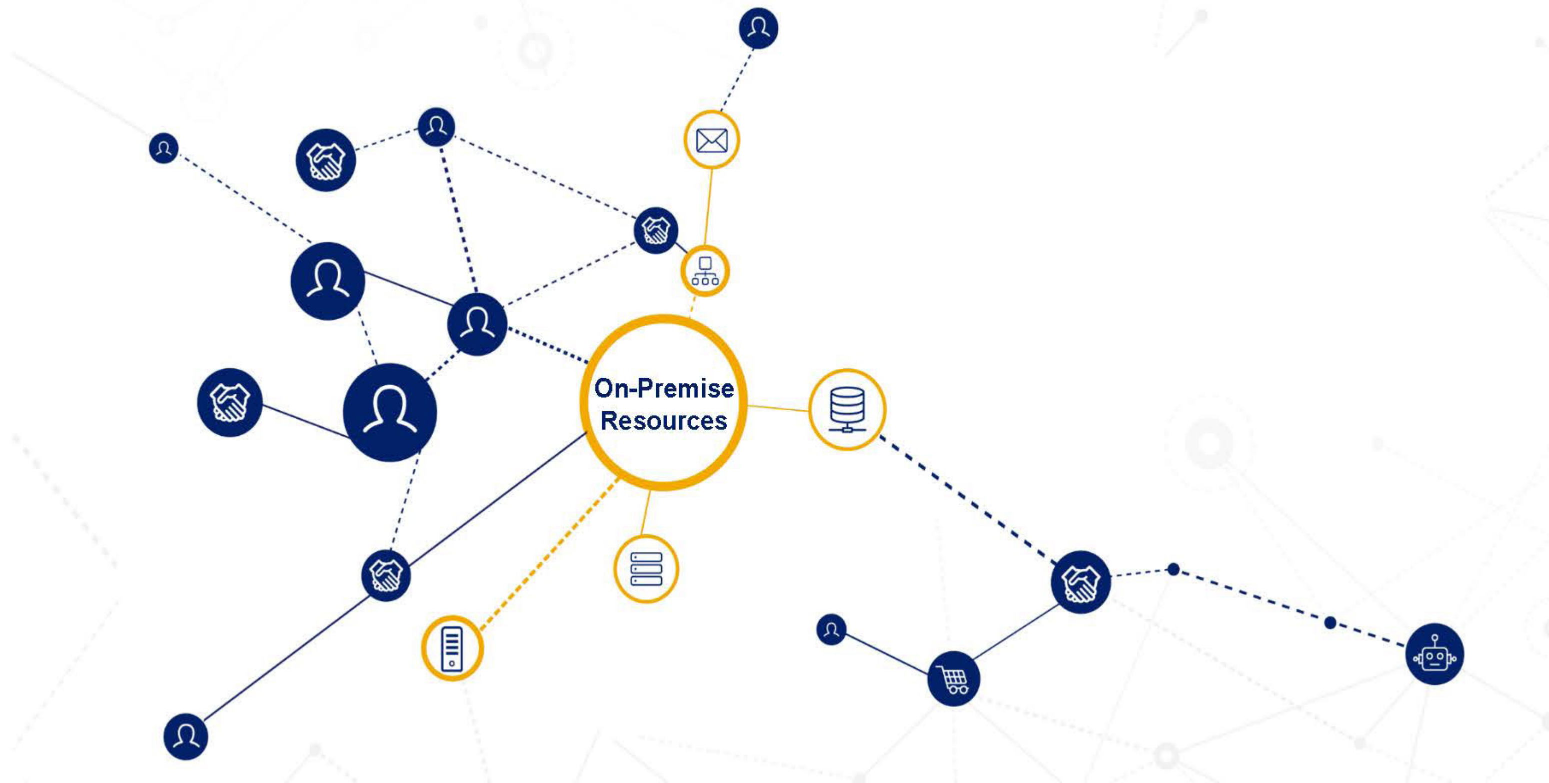
Closing

Topics

1. Starting simple is more important than you think.
2. Why Automated Provisioning can provide a false sense of security
3. How to leverage the power of Artificial Intelligence (AI) to
    1. Dramatically improve the outcomes from your identity program
    2. Extend Identity controls to your cloud infrastructure platforms

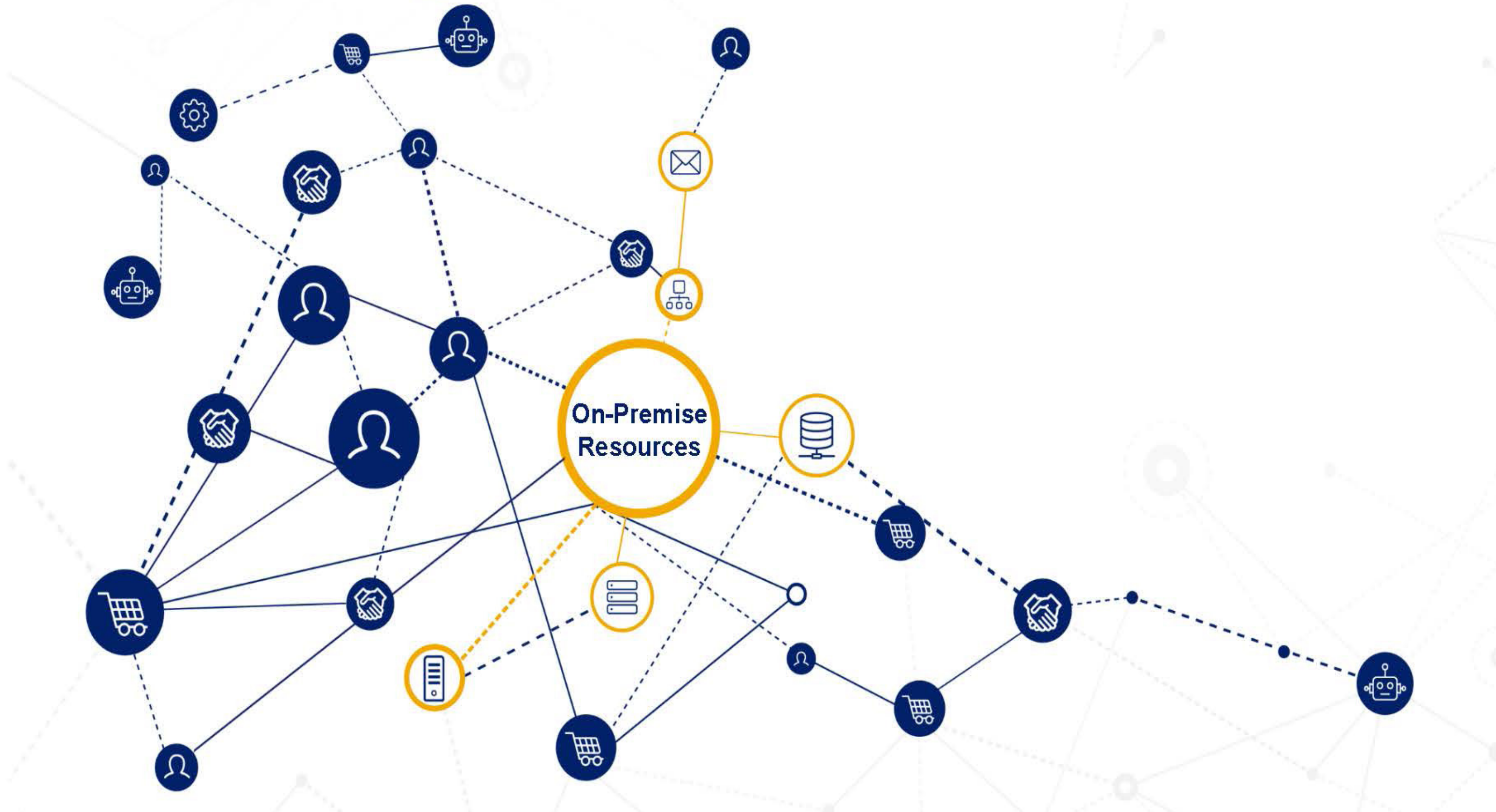
SailPoint

The Challenge

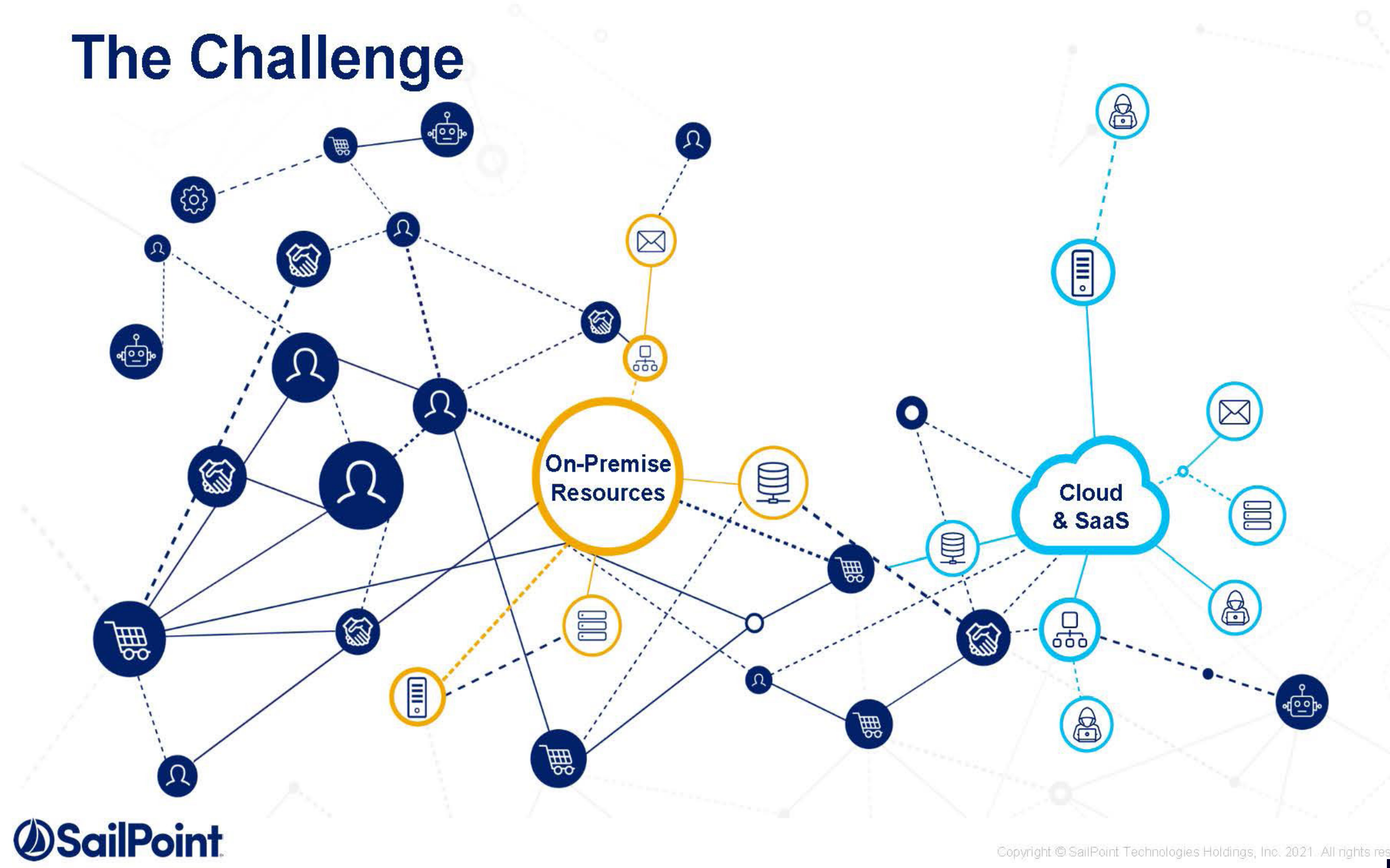


SailPoint

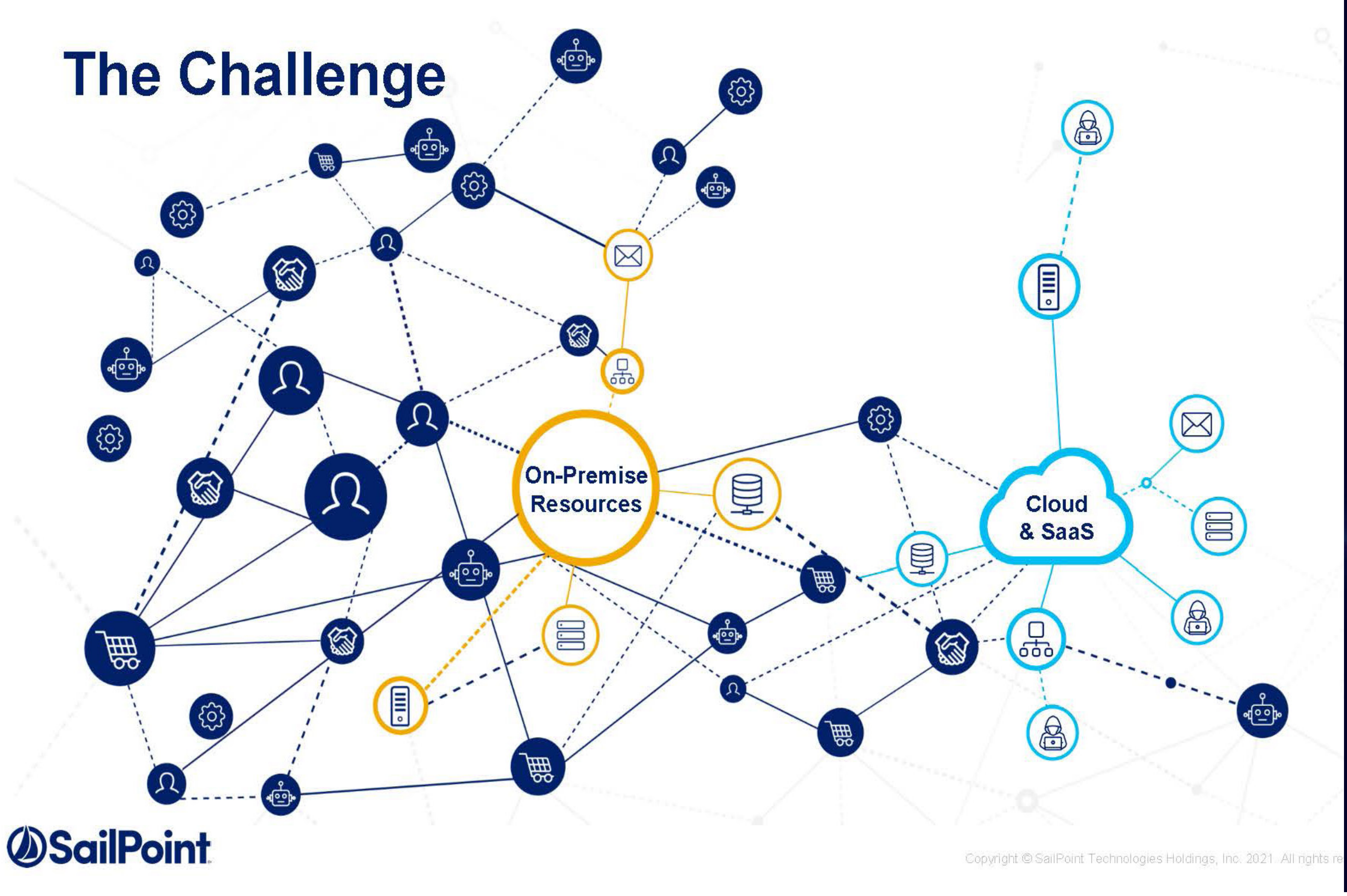
The Challenge



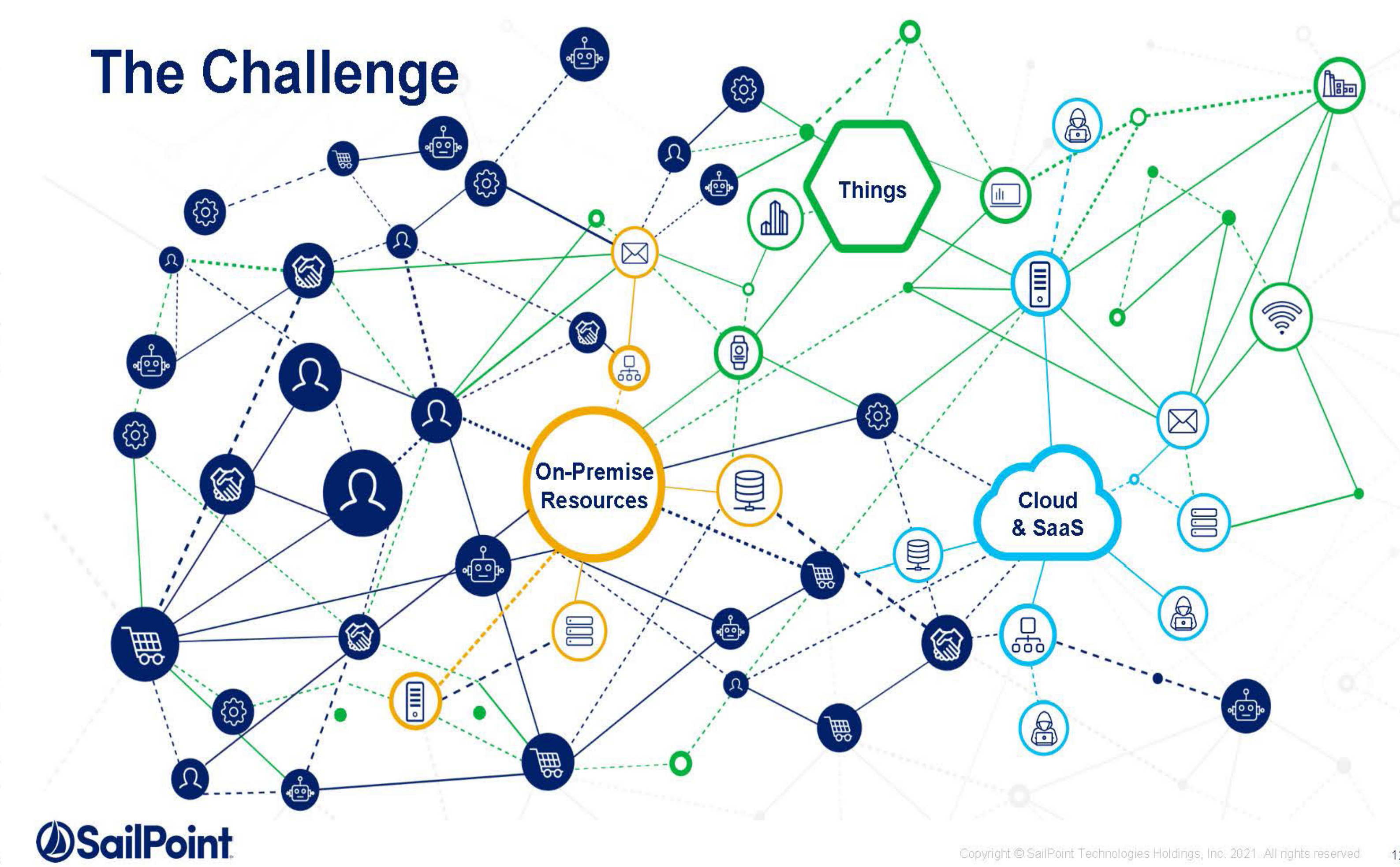
SailPoint



The Challenge



The Challenge



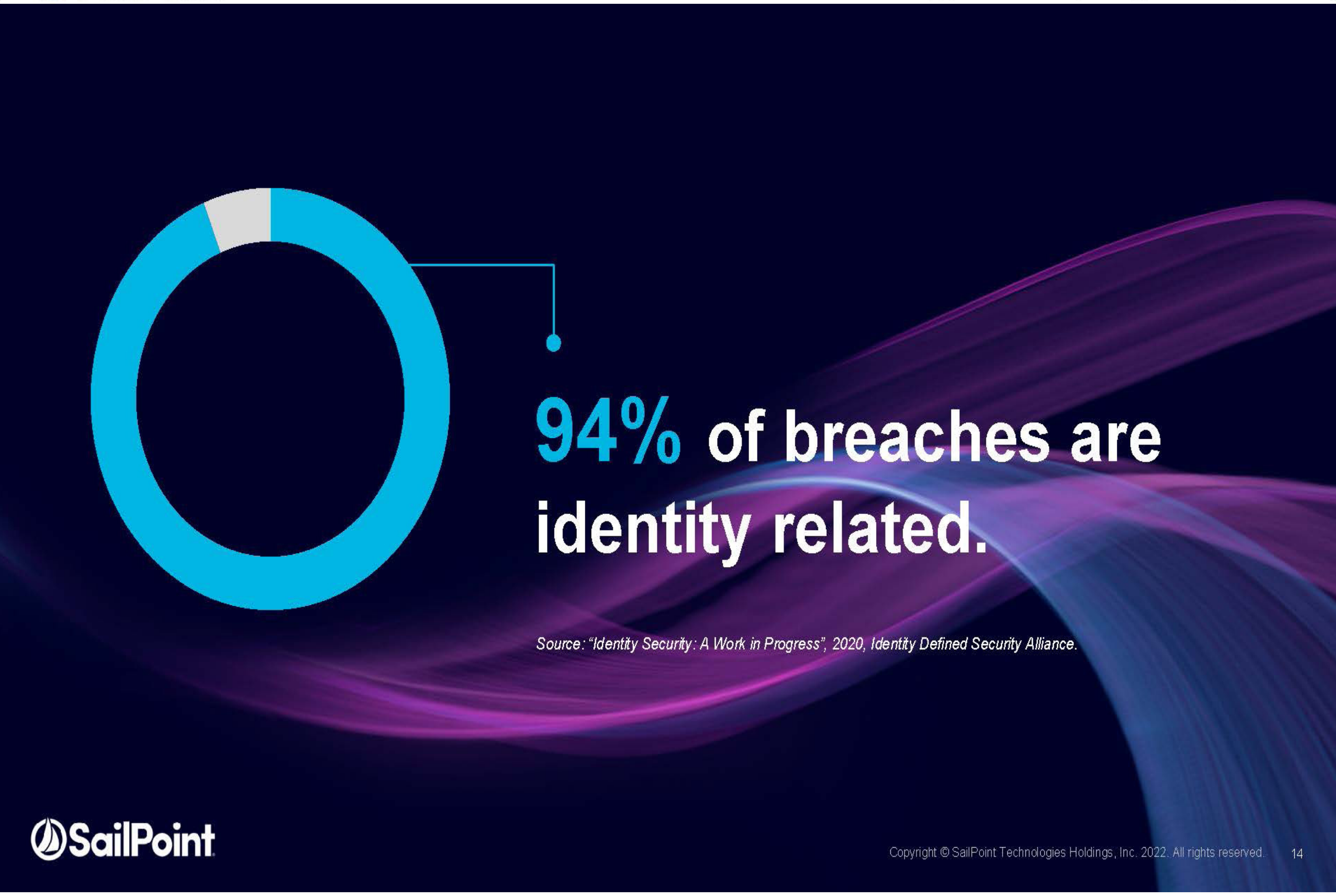
The Challenge

Things

On-Premise Resources

Cloud & SaaS

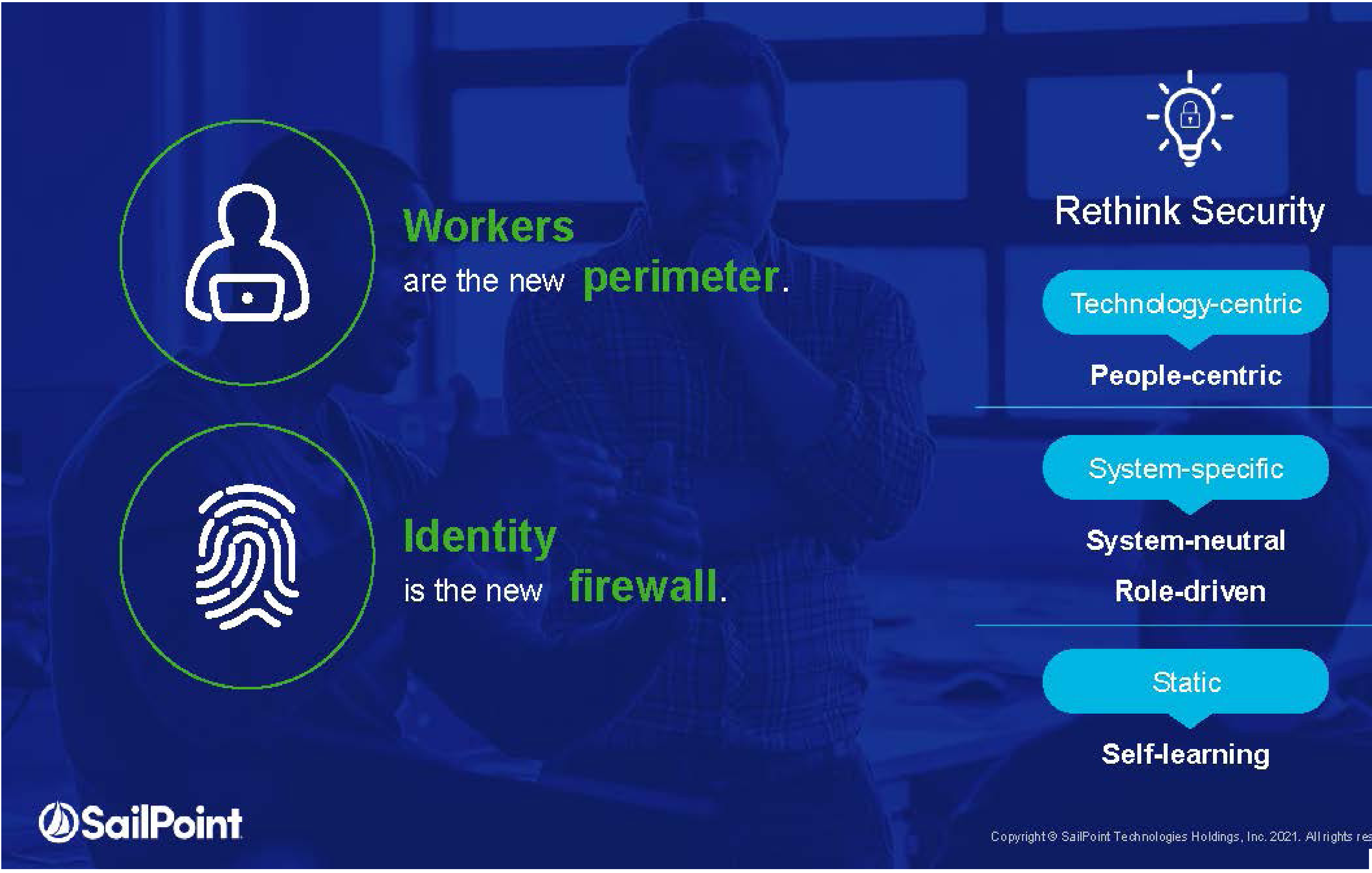
SailPoint



94% of breaches are identity related.

Source: "Identity Security: A Work in Progress", 2020, Identity Defined Security Alliance.

SailPoint



Workers are the new **perimeter**.

Identity is the new **firewall**.

Rethink Security

Technology-centric

People-centric

System-specific

System-neutral

Role-driven

Static

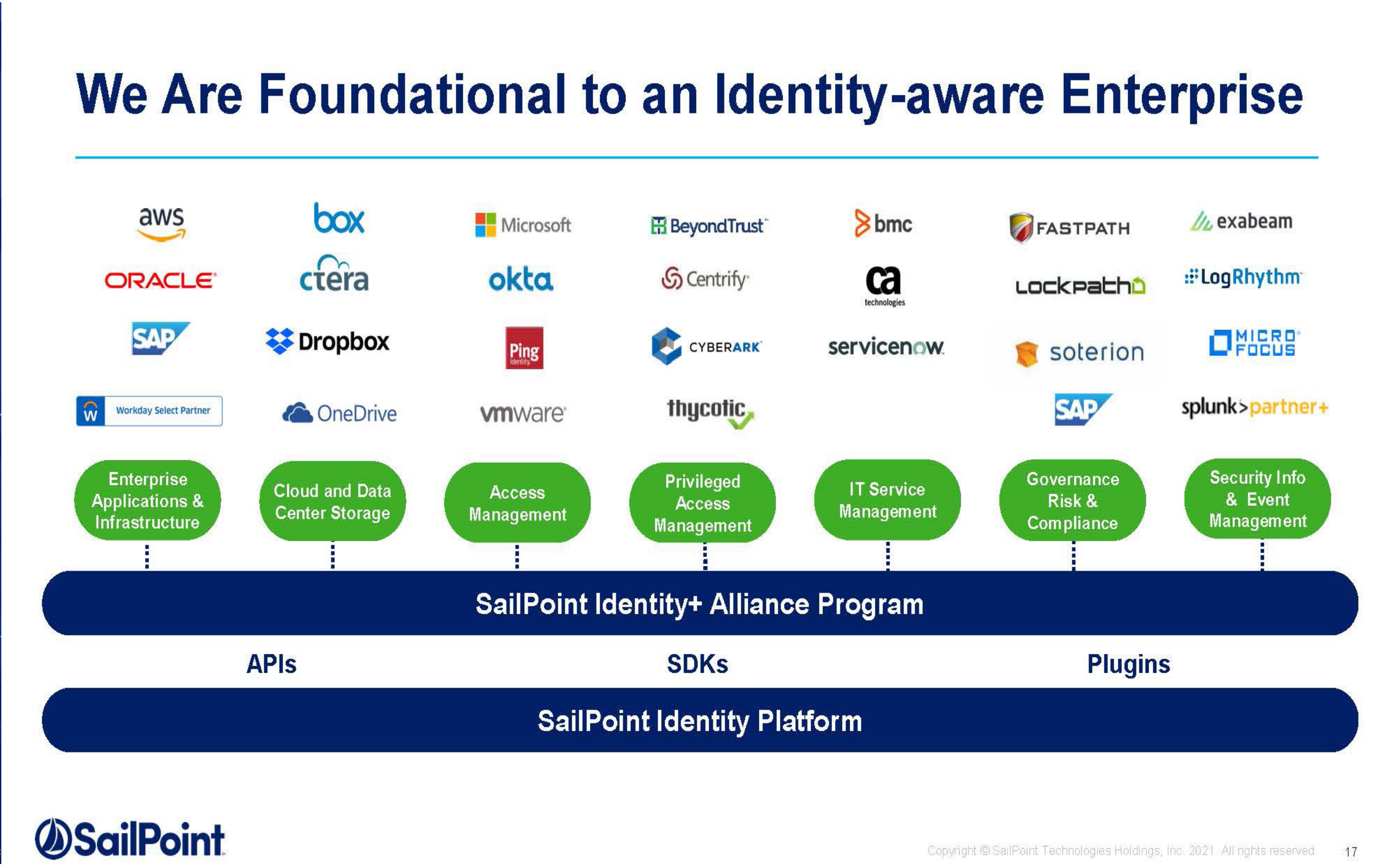
Self-learning

SailPoint

Securely connecting the right people to the right technology has moved **well beyond human capacity**.

SailPoint

16



We Are Foundational to an Identity-aware Enterprise

Enterprise Applications & Infrastructure

Cloud and Data Center Storage

Access Management

Privileged Access Management

IT Service Management

Governance Risk & Compliance

Security Info & Event Management

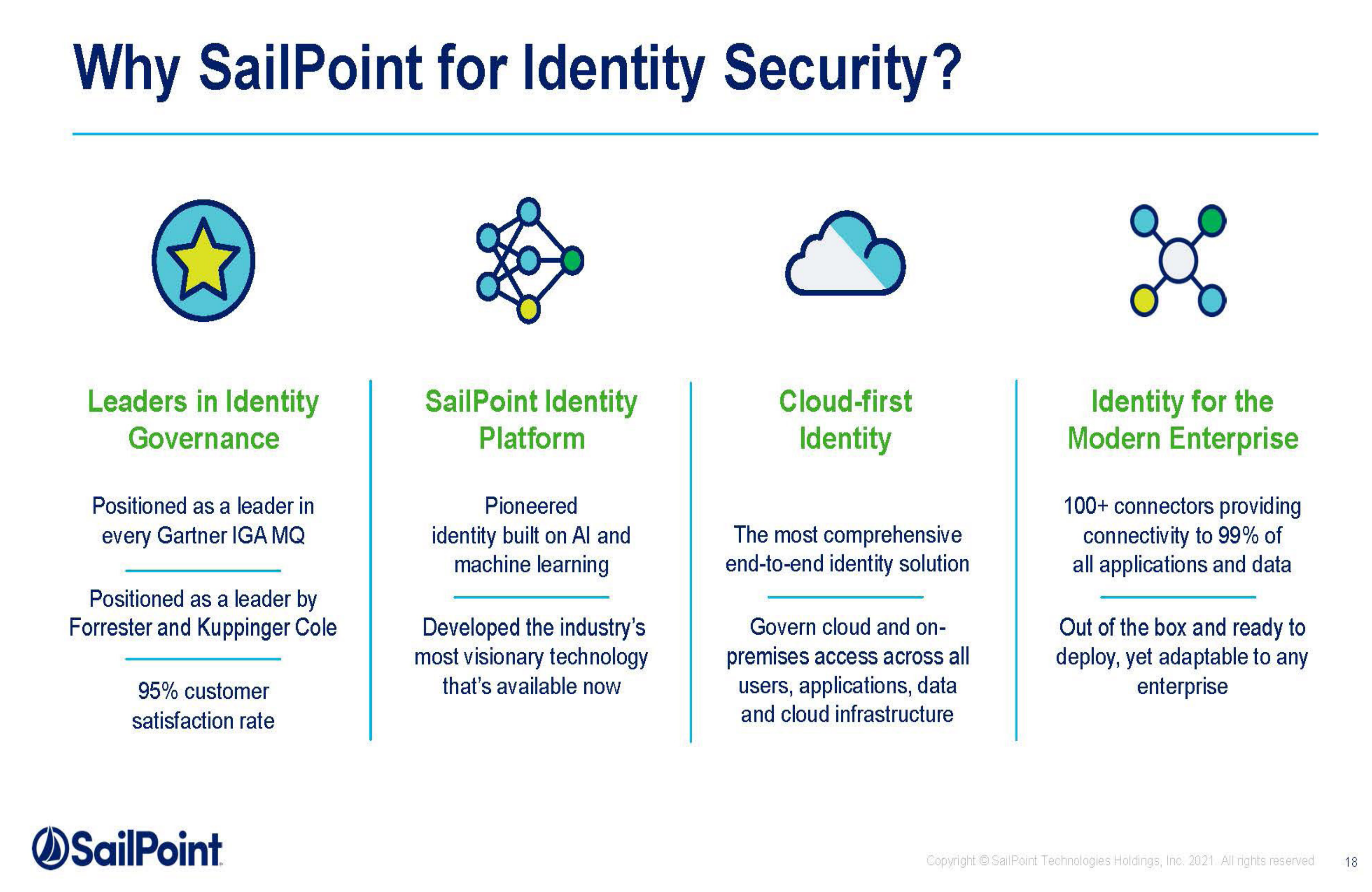
SailPoint Identity+ Alliance Program

APIs

SDKs

Plugins

SailPoint Identity Platform



Why SailPoint for Identity Security?

Leaders in Identity Governance

Positioned as a leader in every Gartner IGA MQ

Positioned as a leader by Forrester and Kuppinger Cole

95% customer satisfaction rate

SailPoint Identity Platform

Pioneered identity built on AI and machine learning

Developed the industry's most visionary technology that's available now

Cloud-first Identity

The most comprehensive end-to-end identity solution

Govern cloud and on-premises access across all users, applications, data and cloud infrastructure

Identity for the Modern Enterprise

100+ connectors providing connectivity to 99% of all applications and data

Out of the box and ready to deploy, yet adaptable to any enterprise

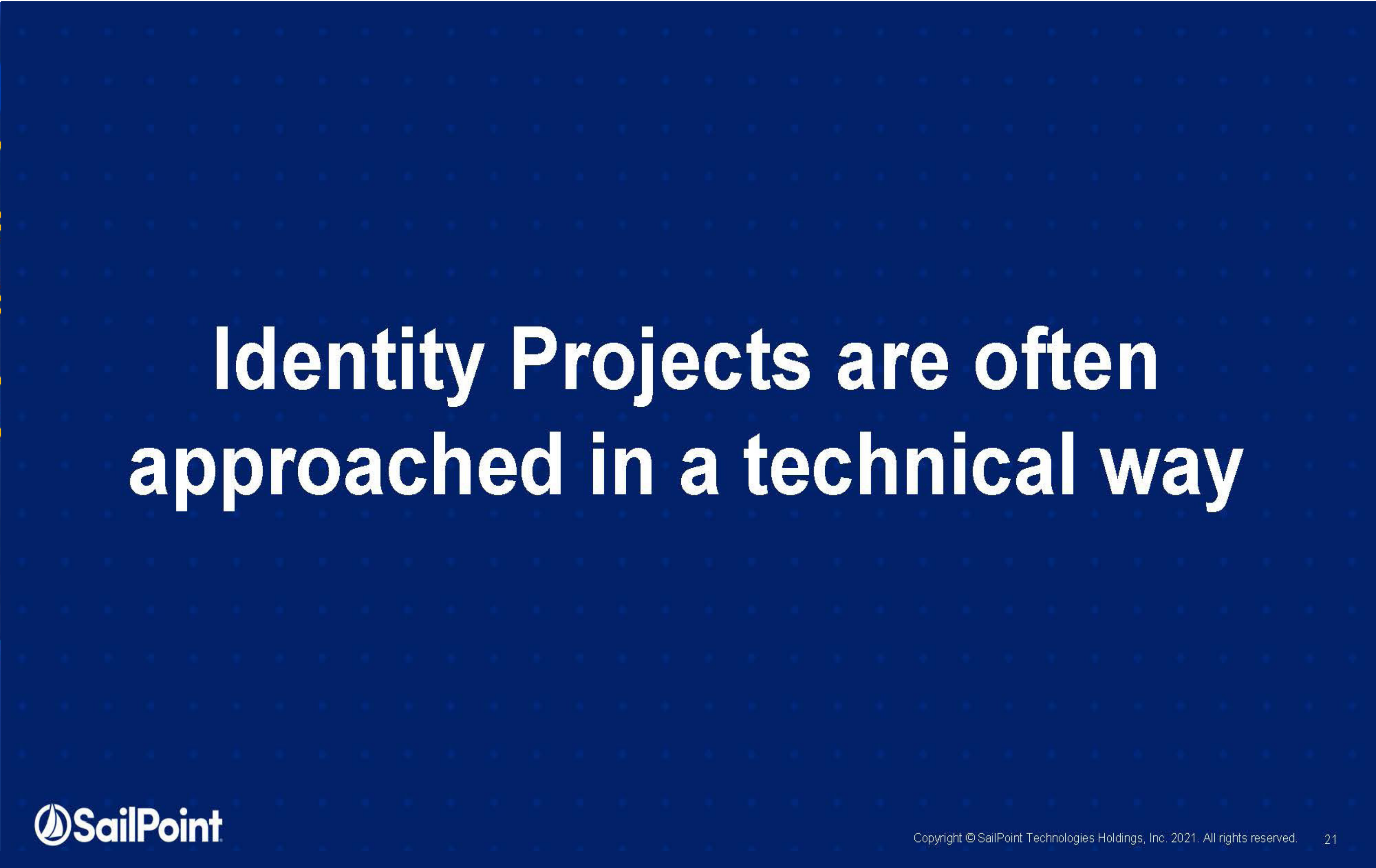
Topics and Discussions

SailPoint

Starting simple is more important than you think

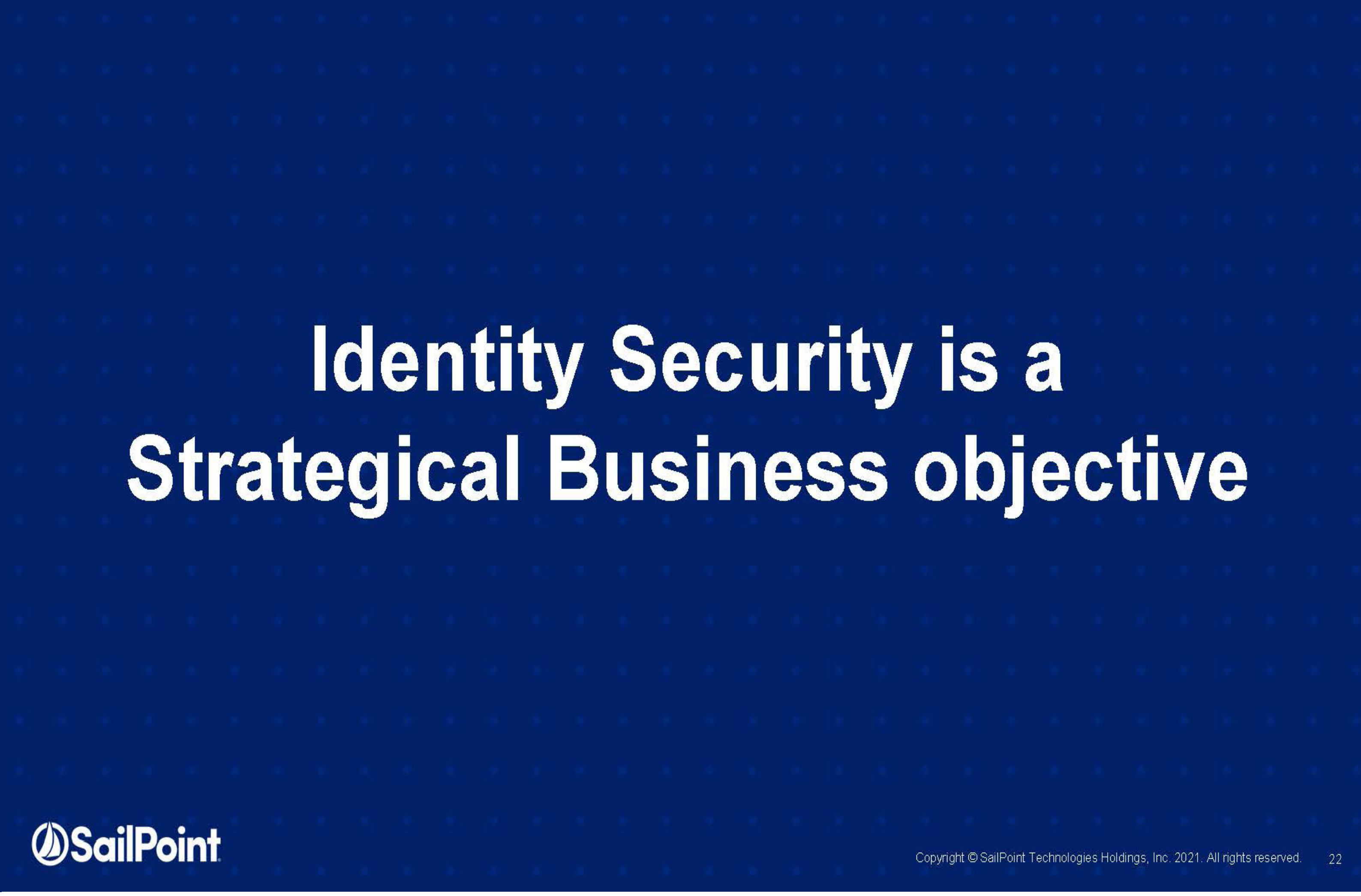
There is more business value in a simple foundation than many realize

SailPoint



Identity Projects are often approached in a technical way

SailPoint



Identity Security is a Strategical Business objective

SailPoint

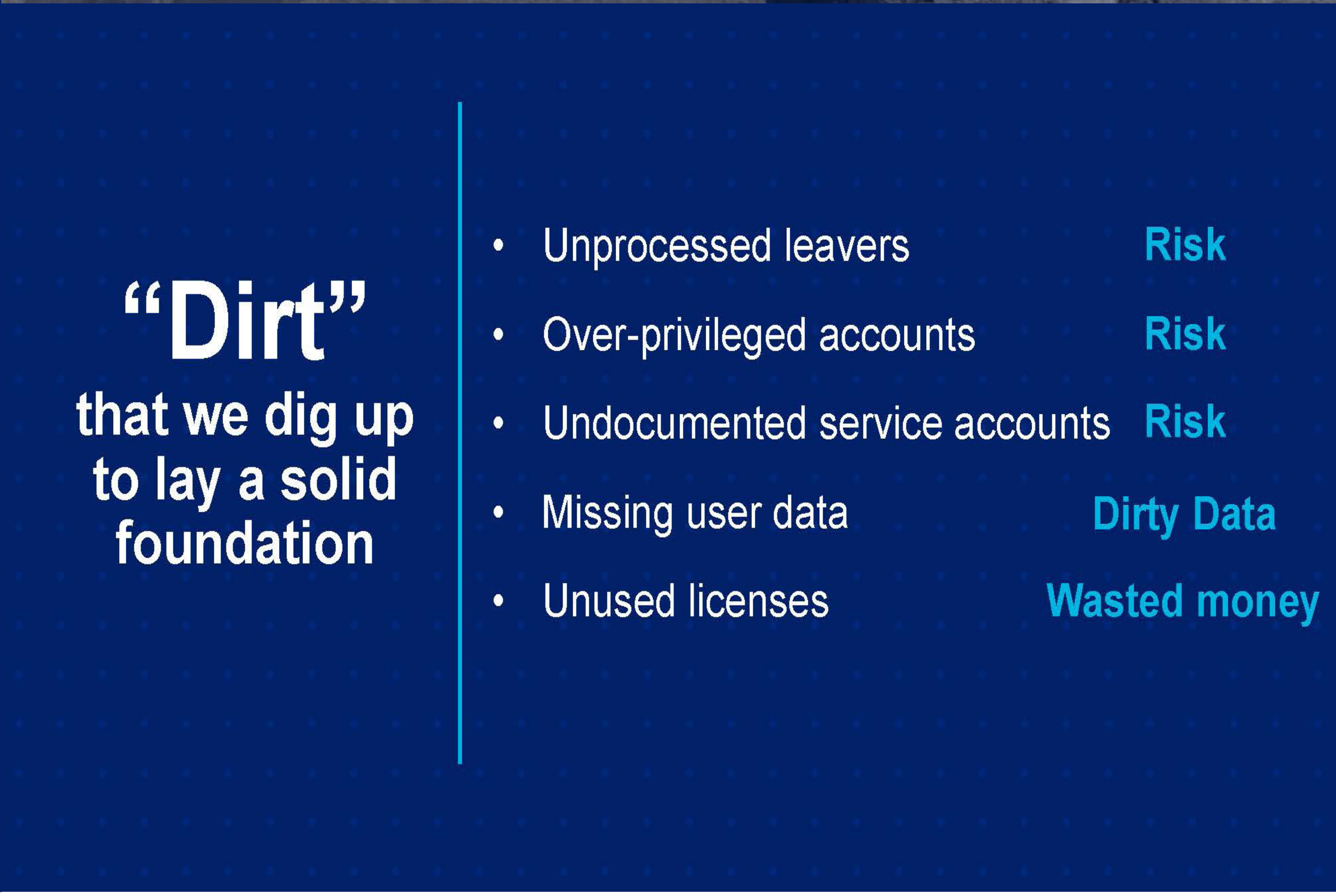
We start by laying a solid foundation

To build a house, you need a strong foundation

To build that foundation, you will need to dig up some dirt…

SailPoint

25

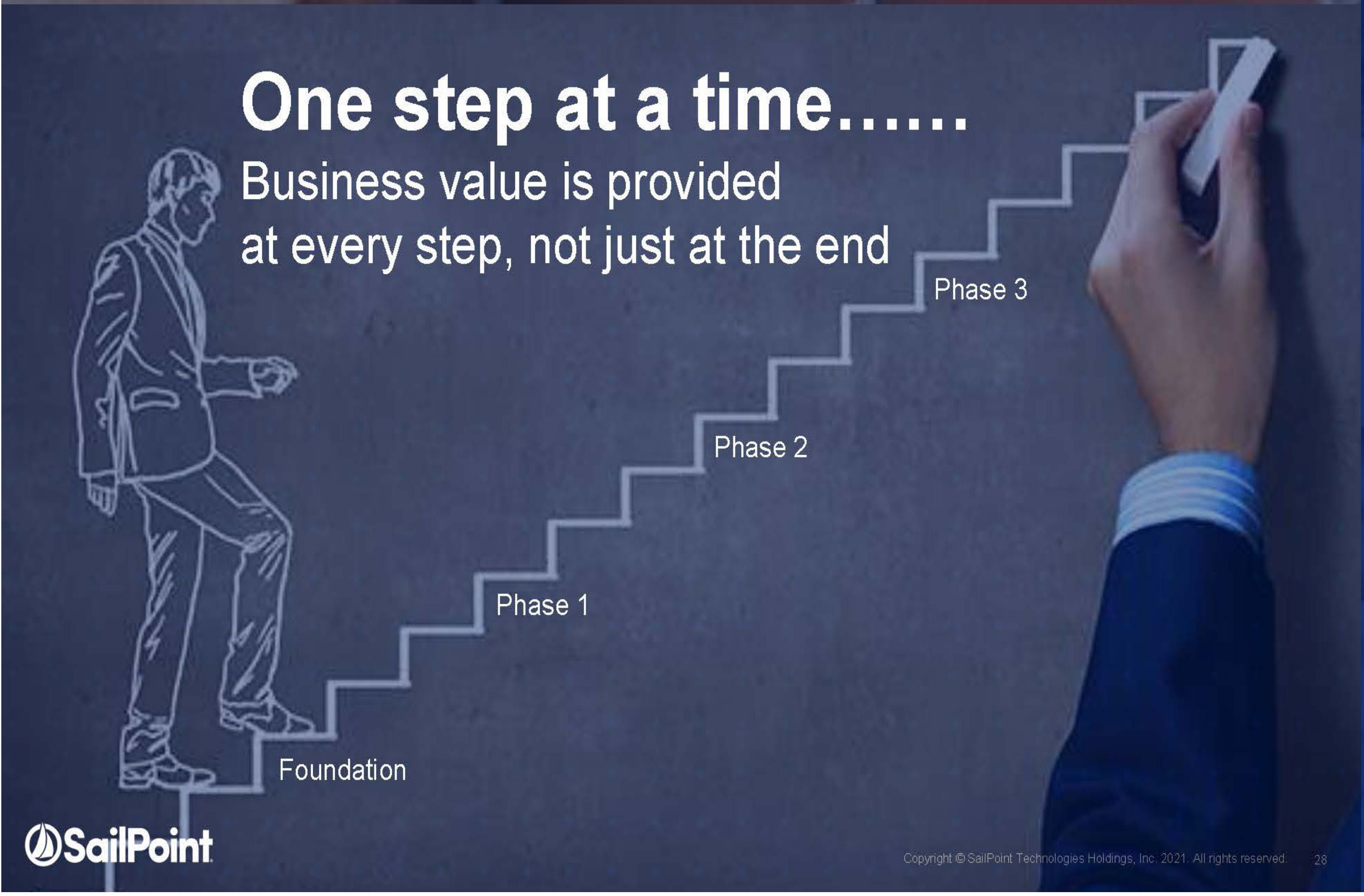


“Dirt” that we dig up to lay a solid foundation

• Unprocessed leavers	Risk
• Over-privileged accounts	Risk
• Undocumented service accounts	Risk
• Missing user data	Dirty Data
• Unused licenses	Wasted money

Every Identity program needs a strong foundation before you build the walls

SailPoint



One step at a time……

Business value is provided
at every step, not just at the end

Phase 3

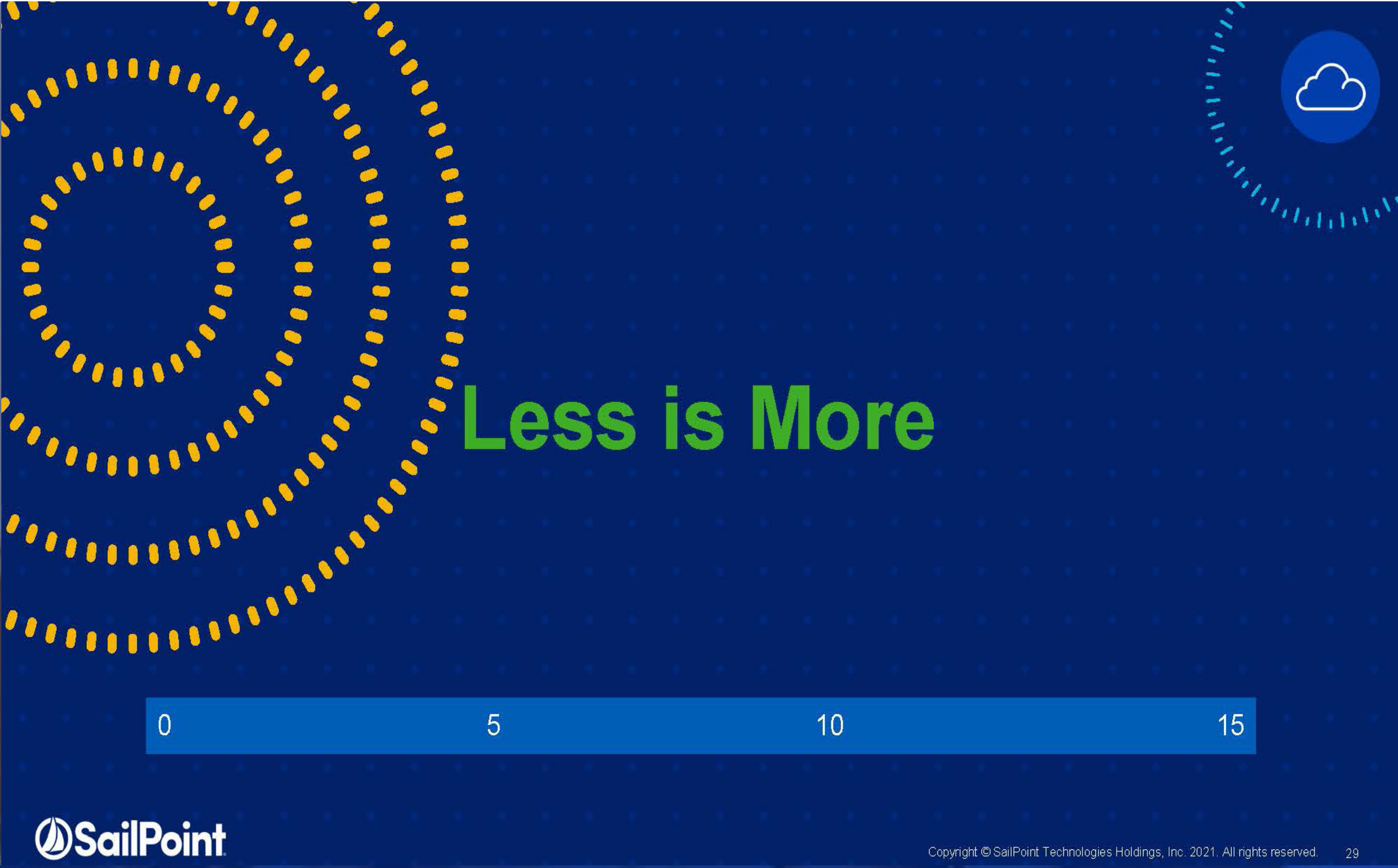
Phase 2

Phase 1

Foundation

SailPoint

28



Less is More

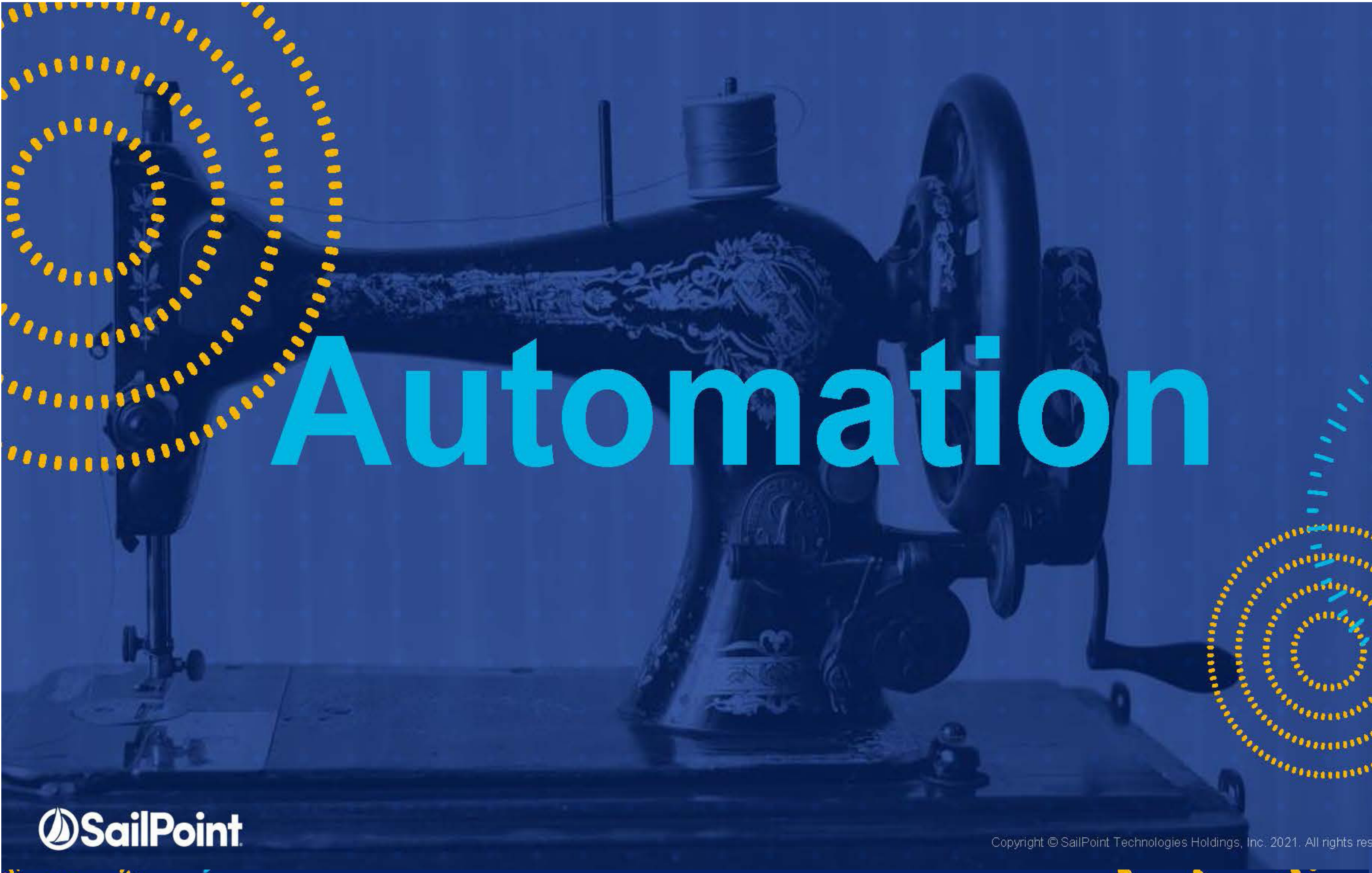
0 5 10 15

SailPoint

29

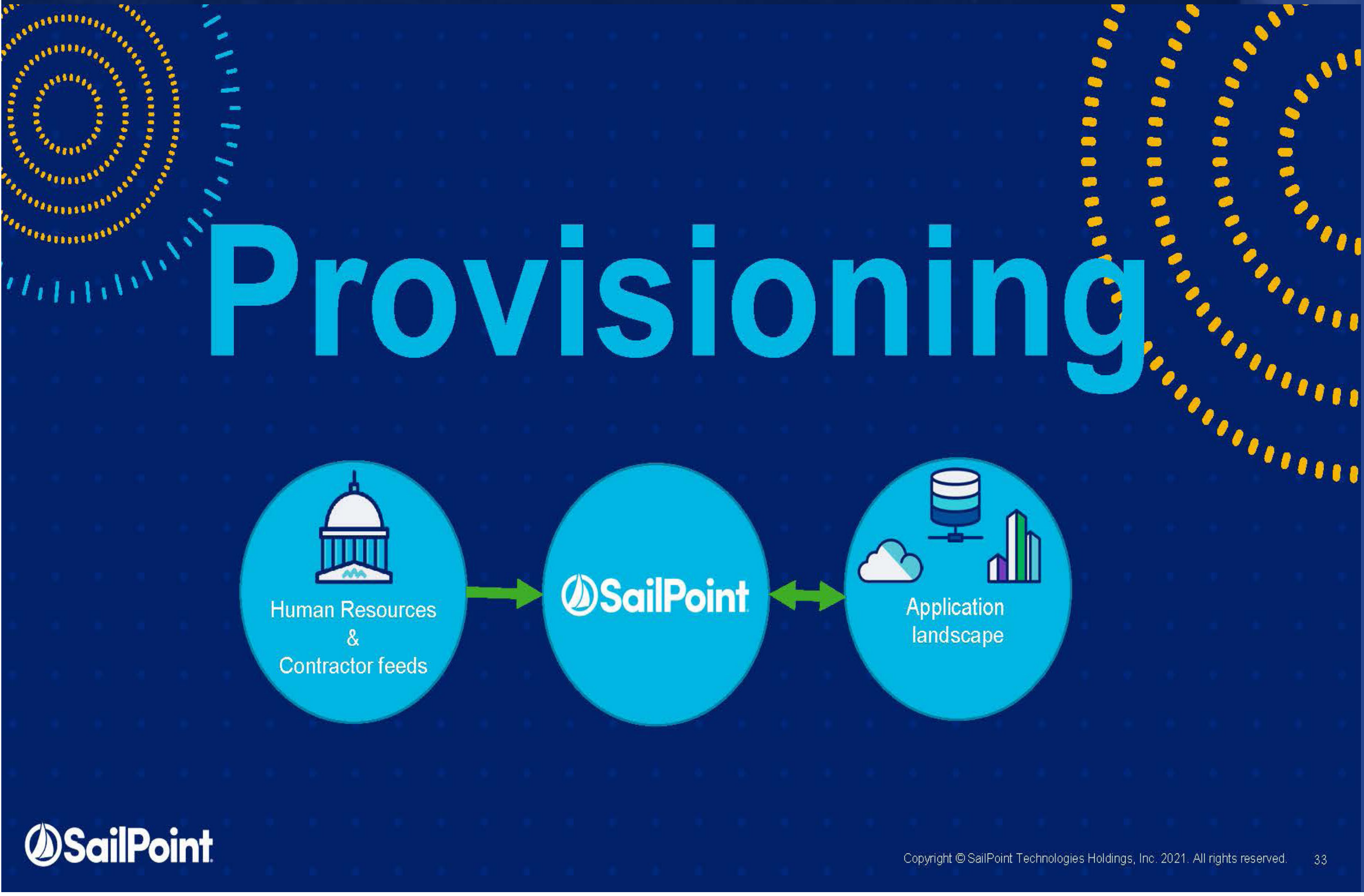
Automated Provisioning can provide a false sense of security

SailPoint



Automation

SailPoint



Provisioning

Human Resources
&
Contractor feeds

SailPoint

Application
landscape

SailPoint

Provisioning

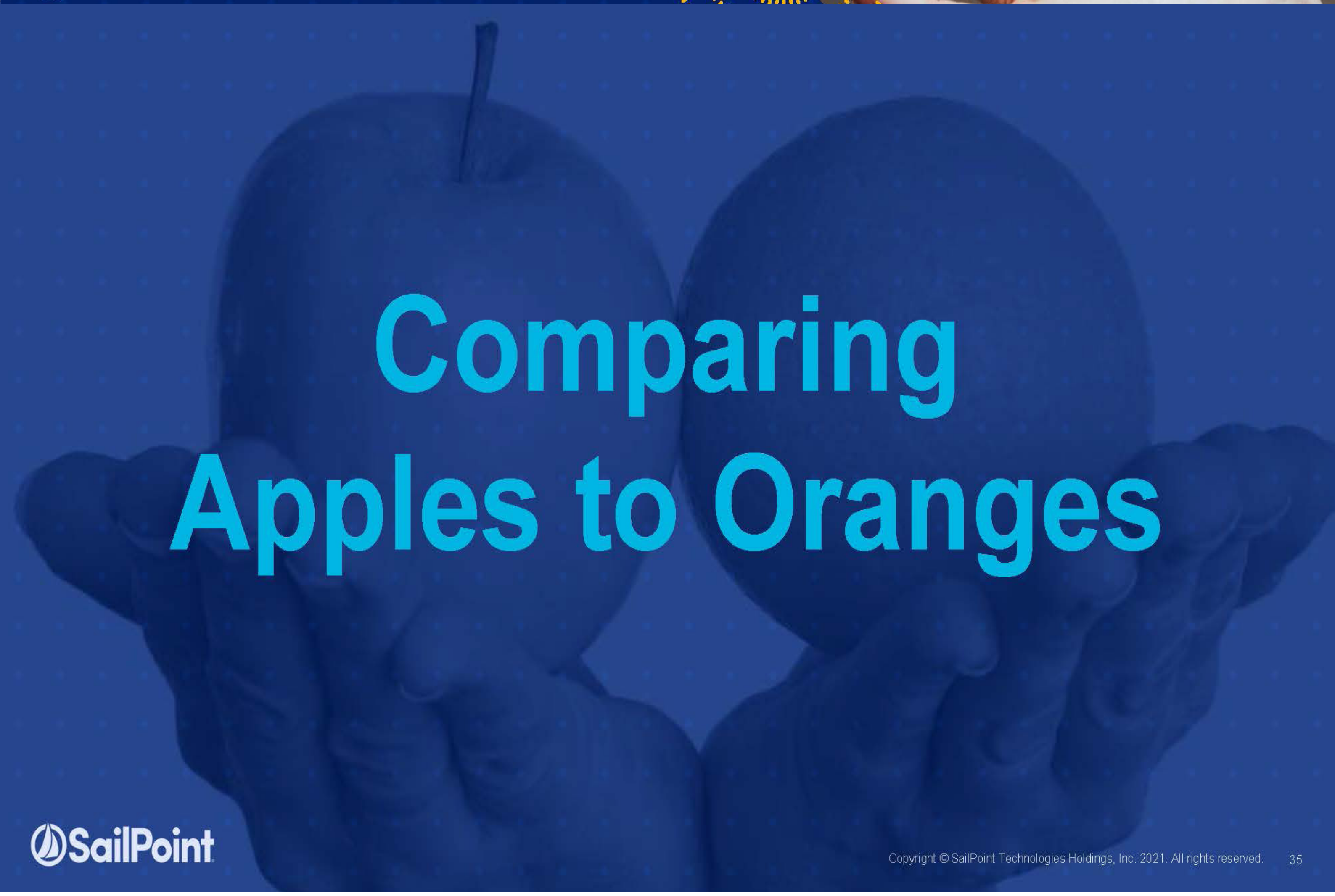
Cost savings and increased productivity

Automatic revocations

Risk reduction

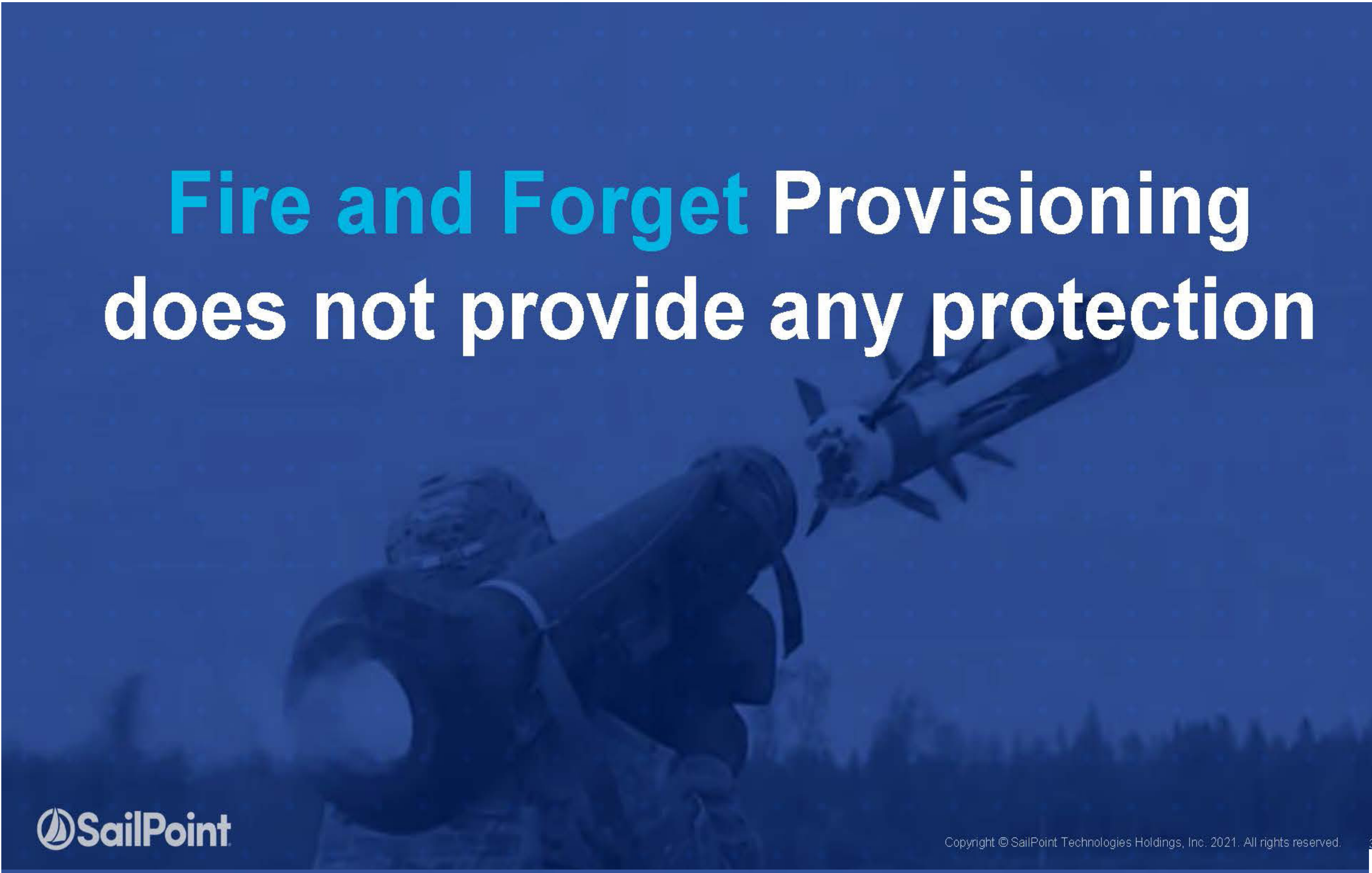
Implementing Least Privileged Access

SailPoint

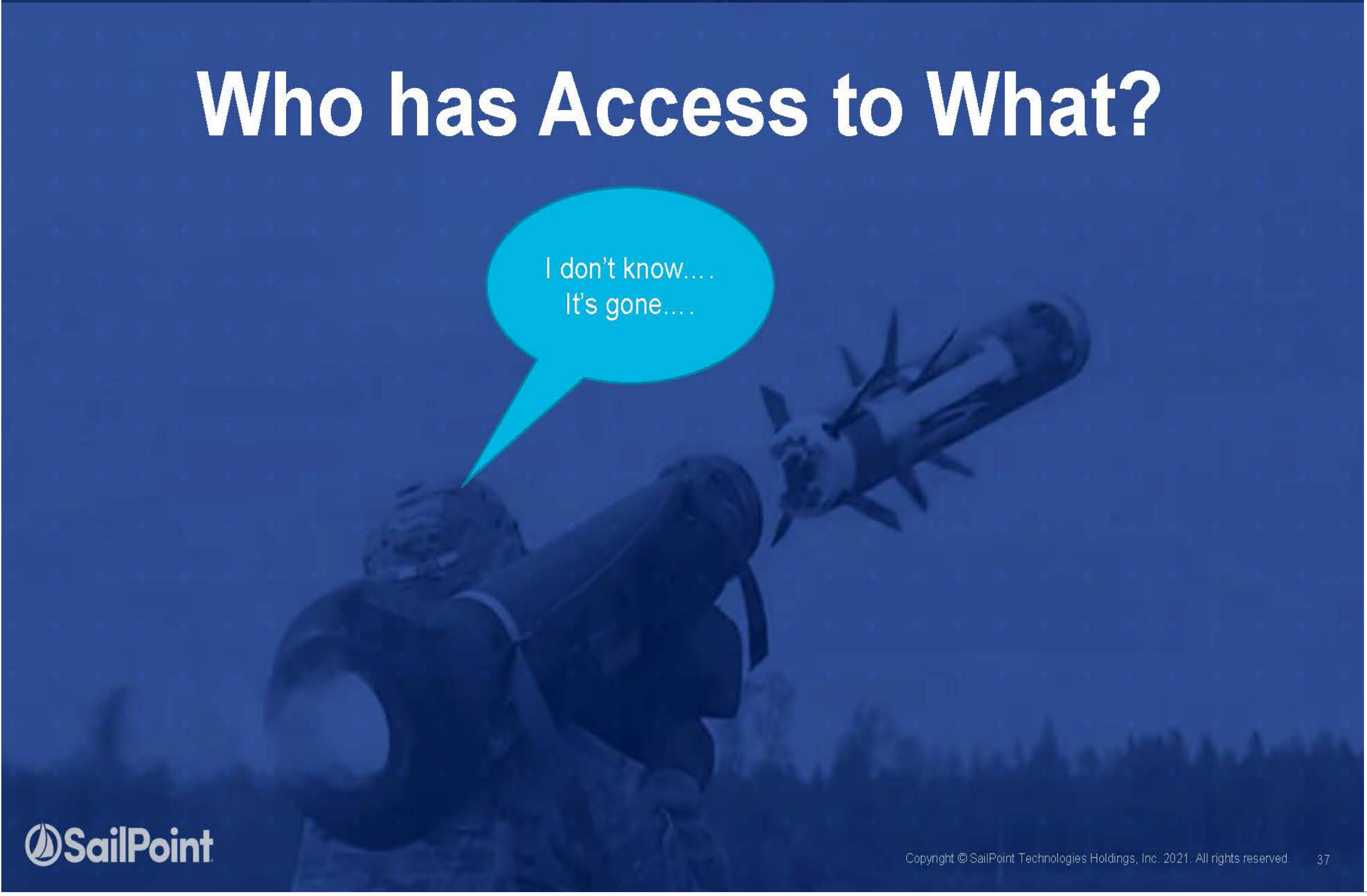


Comparing Apples to Oranges

SailPoint



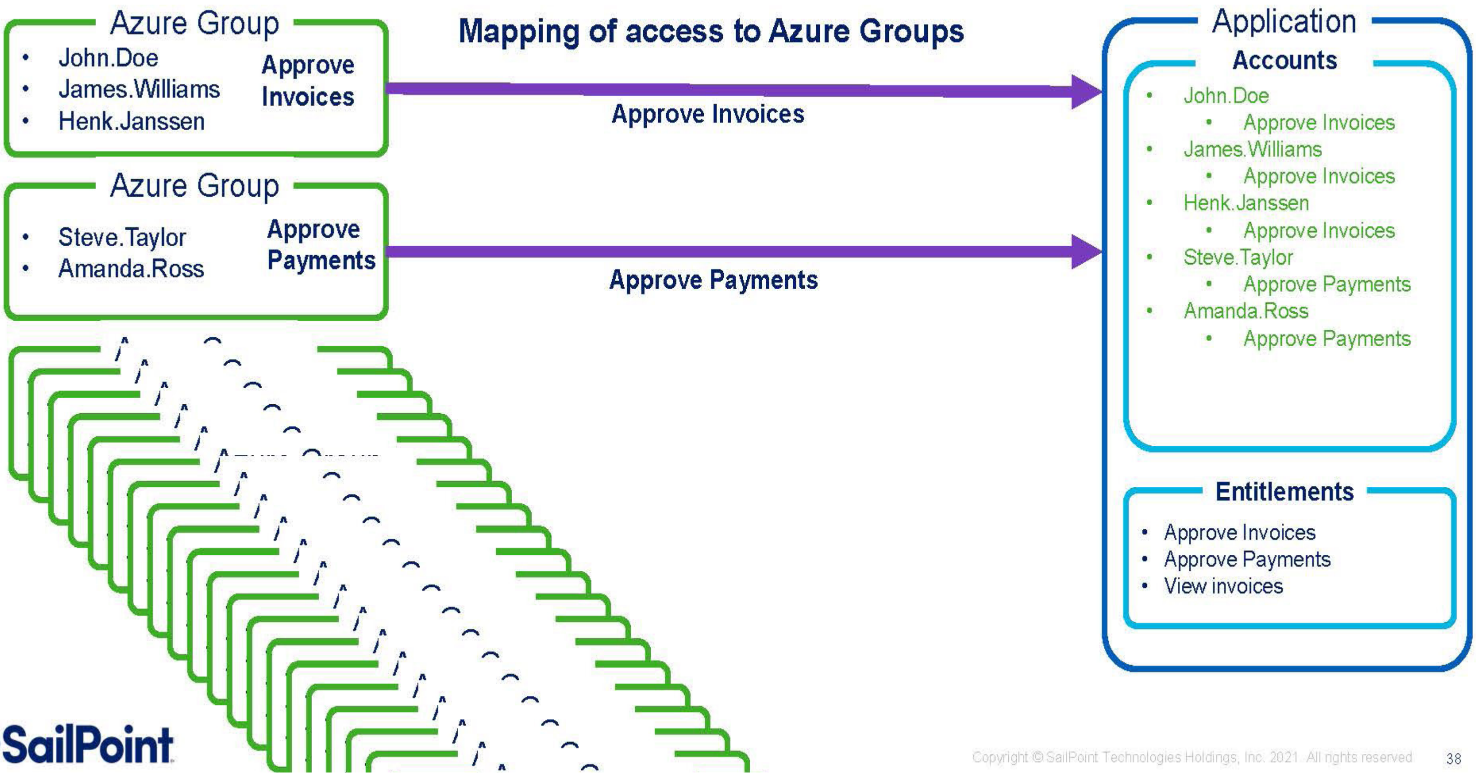
Fire and Forget Provisioning does not provide any protection



Who has Access to What?

I don't know….
It's gone….
SailPoint

Fire and Forget example



Mapping of access to Azure Groups

Azure Group

- John.Doe
- James.Williams
- Henk.Janssen

Approve Invoices

Approve Invoices

Azure Group

- Steve.Taylor
- Amanda.Ross

Approve Payments

Approve Payments

Application

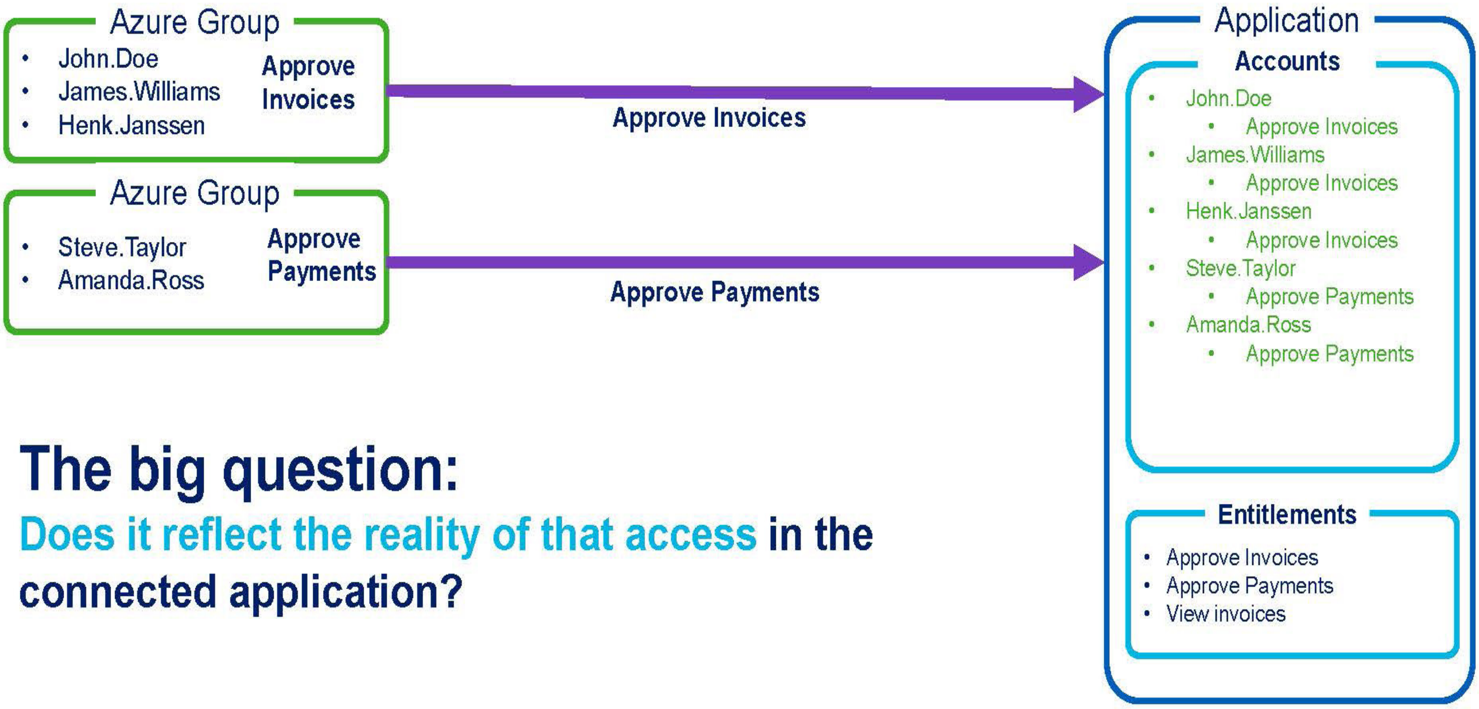
Accounts

- John.Doe
  - Approve Invoices
- James.Williams
  - Approve Invoices
- Henk.Janssen
  - Approve Invoices
- Steve.Taylor
  - Approve Payments
- Amanda.Ross
  - Approve Payments

Entitlements

- Approve Invoices
- Approve Payments
- View invoices

Fire and Forget example



Azure Group

- John.Doe
- James.Williams
- Henk.Janssen

Approve Invoices

Approve Invoices

Azure Group

- Steve.Taylor
- Amanda.Ross

Approve Payments

Approve Payments

Application

Accounts

- John.Doe
  - Approve Invoices
- James.Williams
  - Approve Invoices
- Henk.Janssen
  - Approve Invoices
- Steve.Taylor
  - Approve Payments
- Amanda.Ross
  - Approve Payments

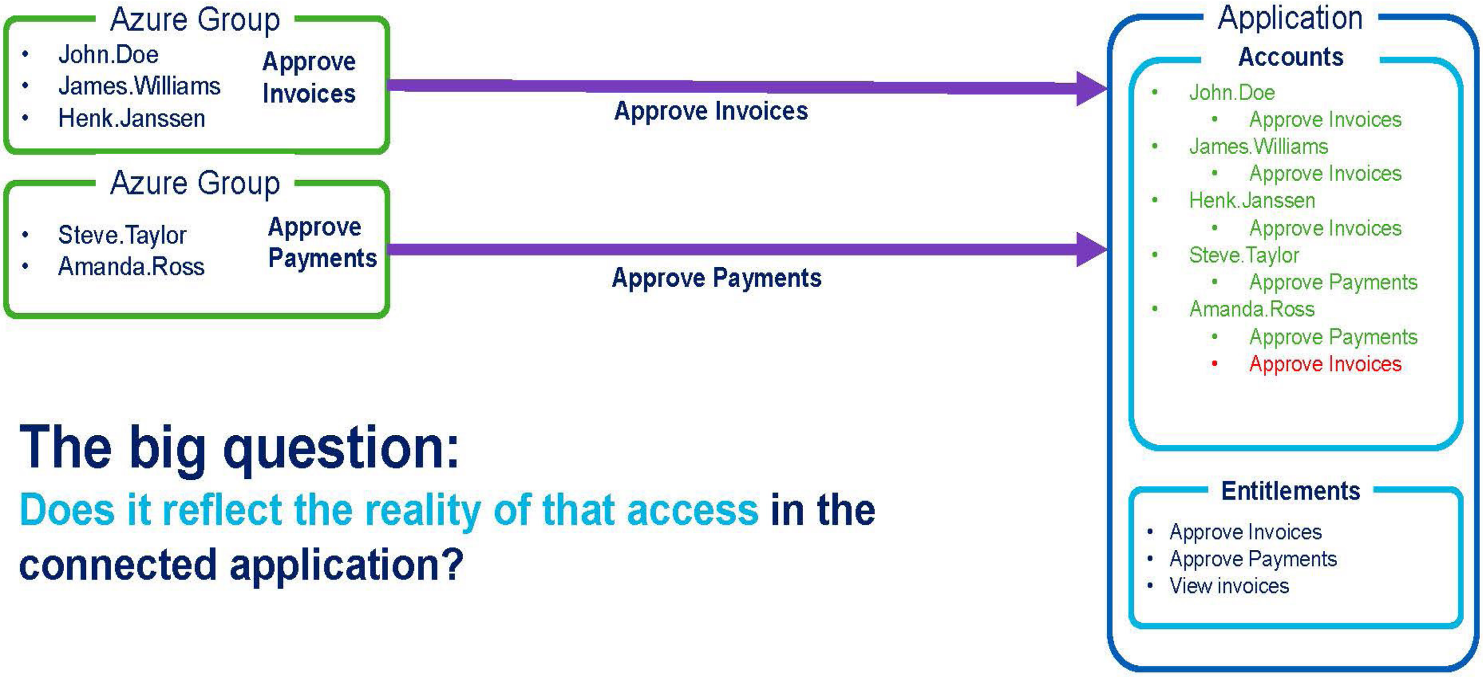
Entitlements

- Approve Invoices
- Approve Payments
- View invoices

The big question:

Does it reflect the reality of that access in the connected application?

Fire and Forget example



Azure Group
- John.Doe
- James.Williams
- Henk.Janssen

Approve Invoices

Azure Group
- Steve.Taylor
- Amanda.Ross

Approve Payments

Approve Invoices

Approve Payments

Application

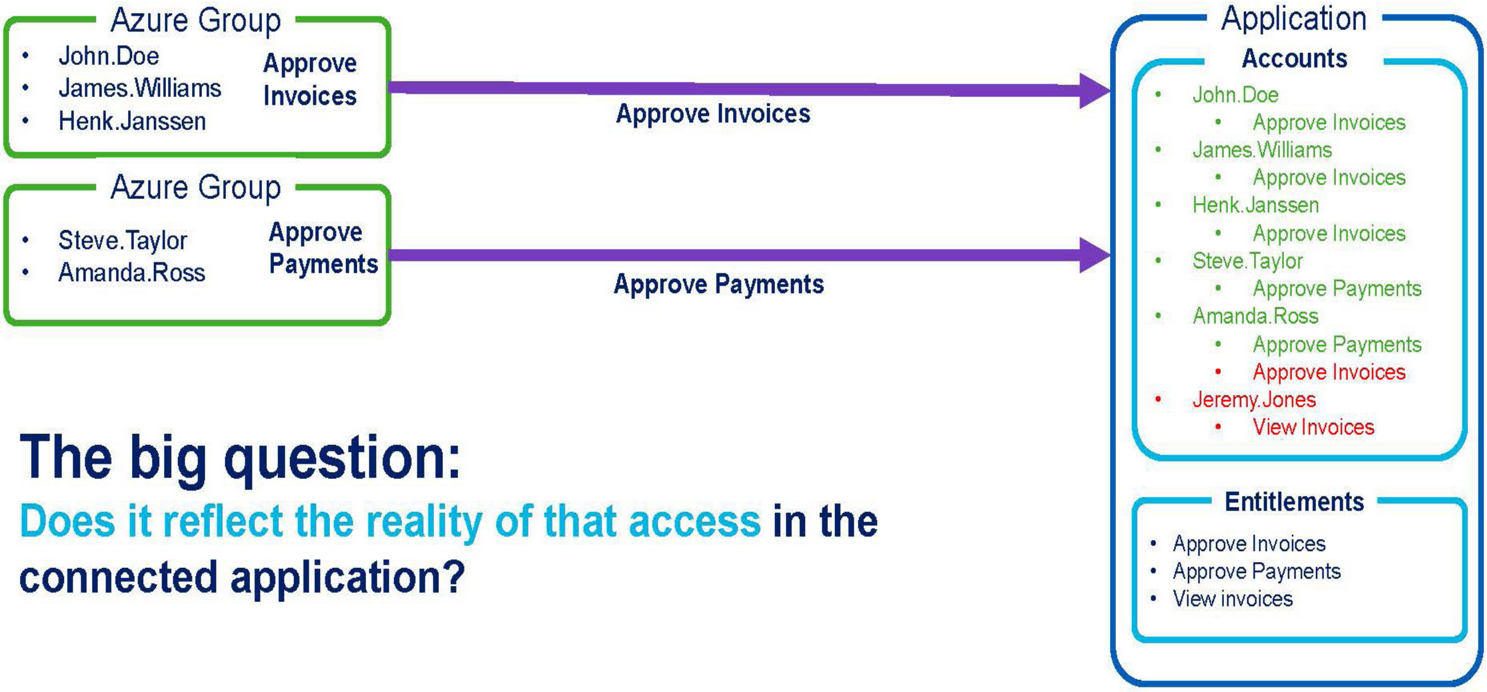
Accounts
- John.Doe
  - Approve Invoices
- James.Williams
  - Approve Invoices
- Henk.Janssen
  - Approve Invoices
- Steve.Taylor
  - Approve Payments
- Amanda.Ross
  - Approve Payments
  - Approve Invoices

Entitlements
- Approve Invoices
- Approve Payments
- View invoices

The big question:

Does it reflect the reality of that access in the connected application?

Fire and Forget example



Azure Group
- John.Doe
- James.Williams
- Henk.Janssen

Approve Invoices

Azure Group
- Steve.Taylor
- Amanda.Ross

Approve Payments

Approve Invoices

Approve Payments

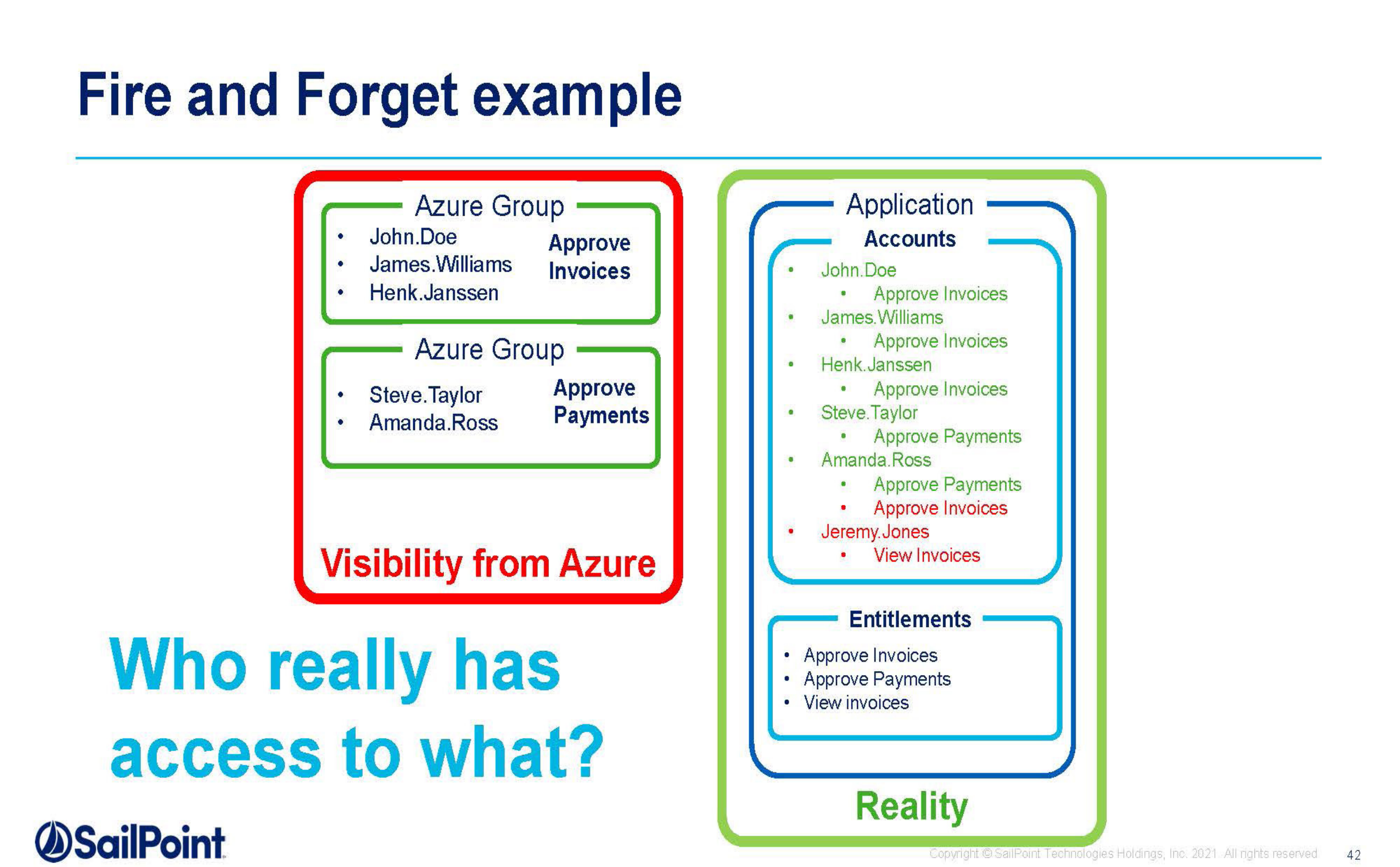
Application

Accounts
- John.Doe
  - Approve Invoices
- James.Williams
  - Approve Invoices
- Henk.Janssen
  - Approve Invoices
- Steve.Taylor
  - Approve Payments
- Amanda.Ross
  - Approve Payments
  - Approve Invoices
- Jeremy.Jones
  - View Invoices

Entitlements
- Approve Invoices
- Approve Payments
- View invoices

The big question:

Does it reflect the reality of that access in the connected application?



Fire and Forget example

Azure Group
- John.Doe
- James.Williams
- Henk.Janssen

Approve Invoices

Azure Group
- Steve.Taylor
- Amanda.Ross

Approve Payments

Visibility from Azure

Who really has access to what?

Application

Accounts
- John.Doe
  - Approve Invoices
- James.Williams
  - Approve Invoices
- Henk.Janssen
  - Approve Invoices
- Steve.Taylor
  - Approve Payments
- Amanda.Ross
  - Approve Payments
  - Approve Invoices
- Jeremy.Jones
  - View Invoices

Entitlements
- Approve Invoices
- Approve Payments
- View invoices

Reality

SailPoint

It provides a False Sense of security

SailPoint

“Who has access to what”

How much visibility do you have today?

SailPoint

Is “just provisioning” good enough?

SailPoint

45

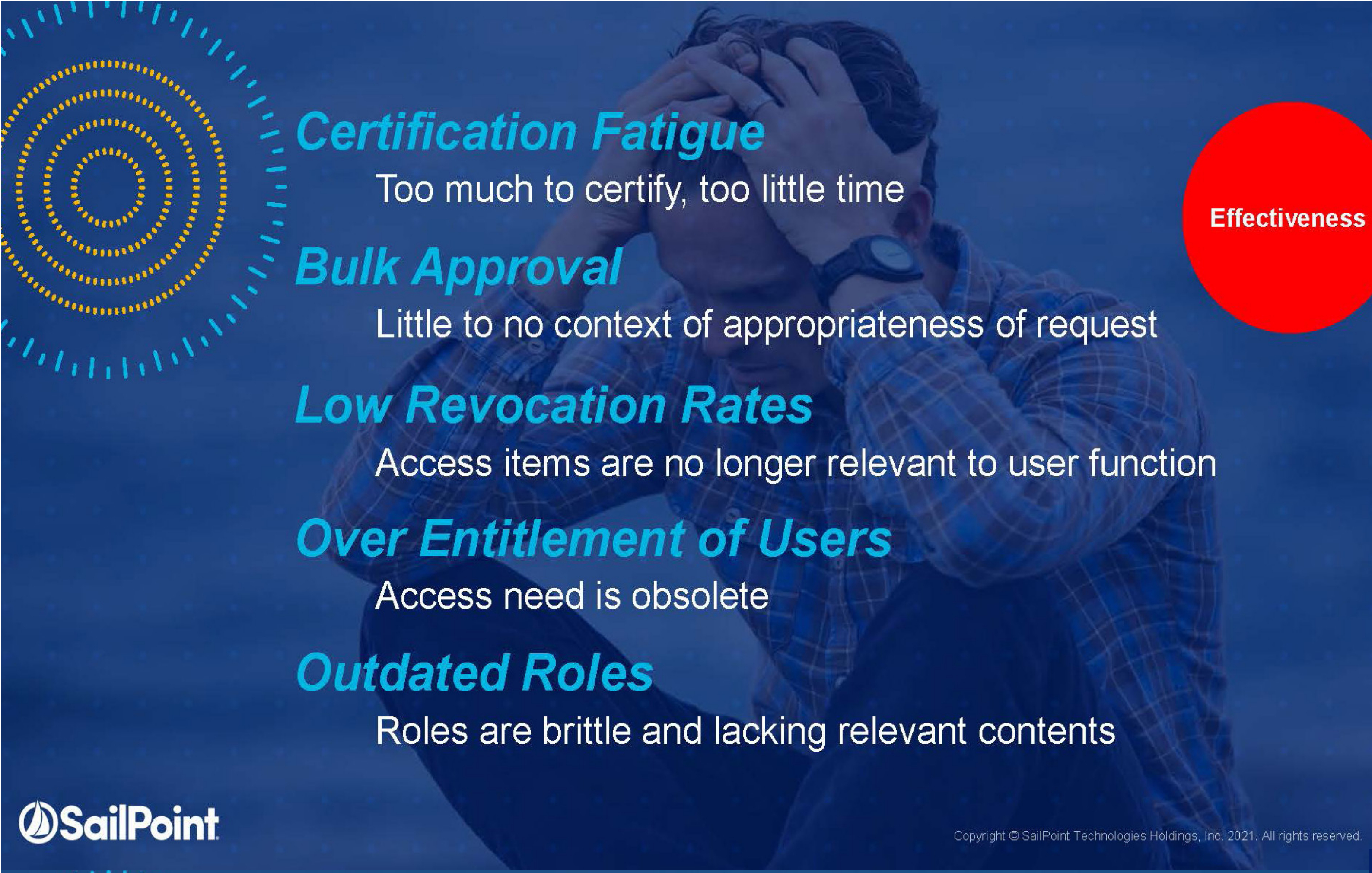
Artificial Intelligence

allows you to take control in complex situations

The majority of companies

Struggle

to stay ahead of the ever changing requirements



Effectiveness

Certification Fatigue

Too much to certify, too little time

Bulk Approval

Little to no context of appropriateness of request

Low Revocation Rates

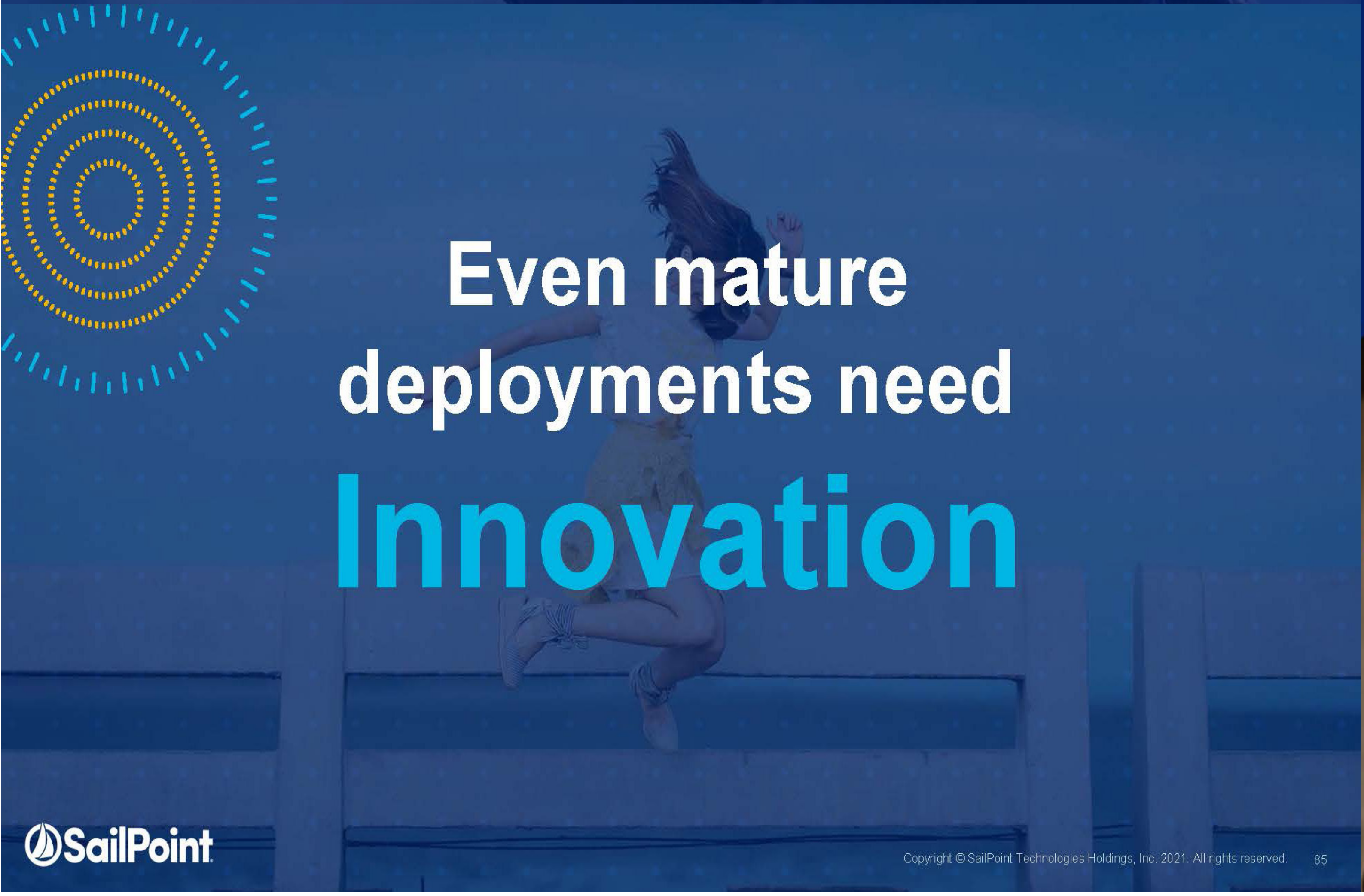
Access items are no longer relevant to user function

Over Entitlement of Users

Access need is obsolete

Outdated Roles

Roles are brittle and lacking relevant contents



Even mature deployments need **Innovation**

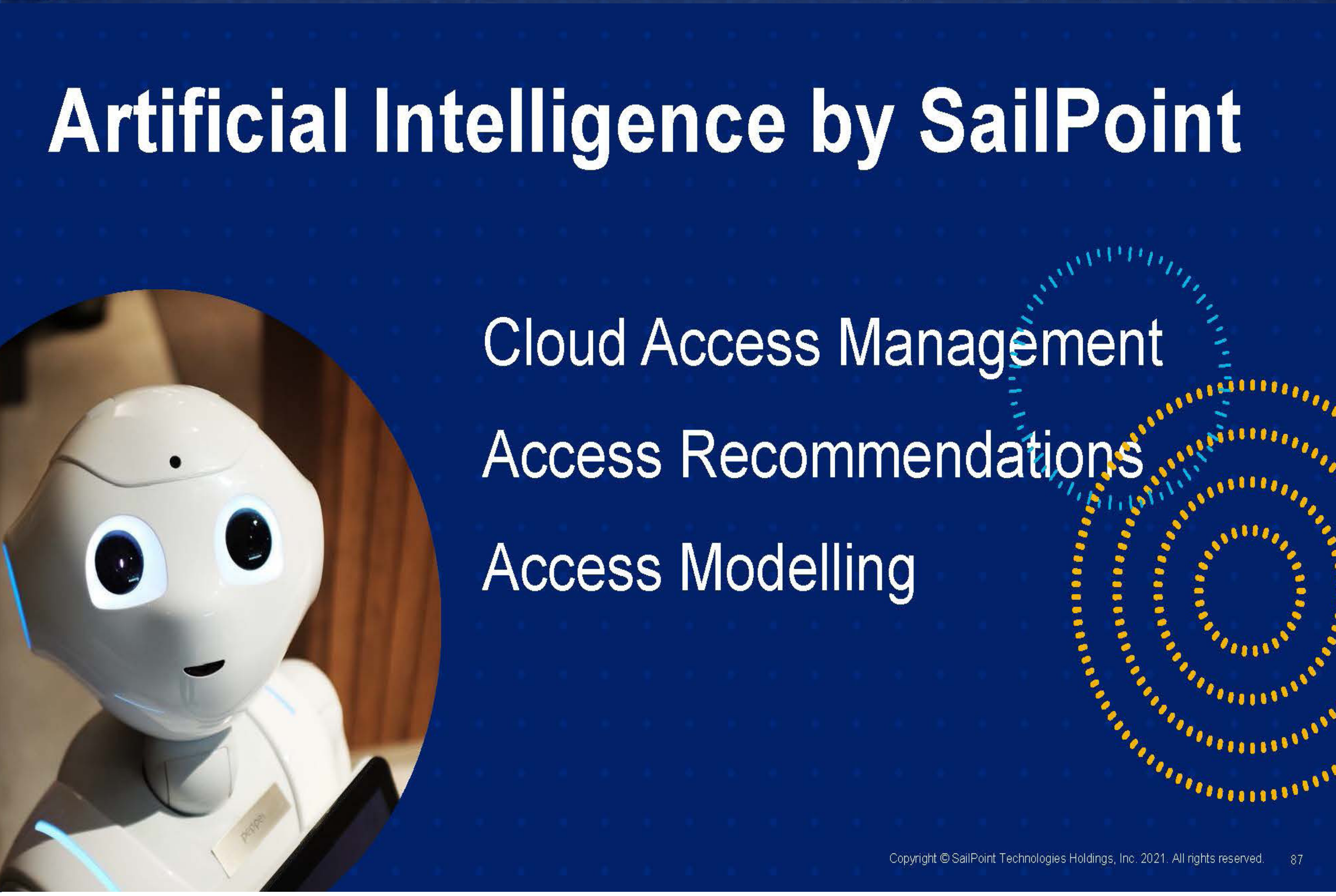
85

We need

Artificial Intelligence

SailPoint

Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved. 86



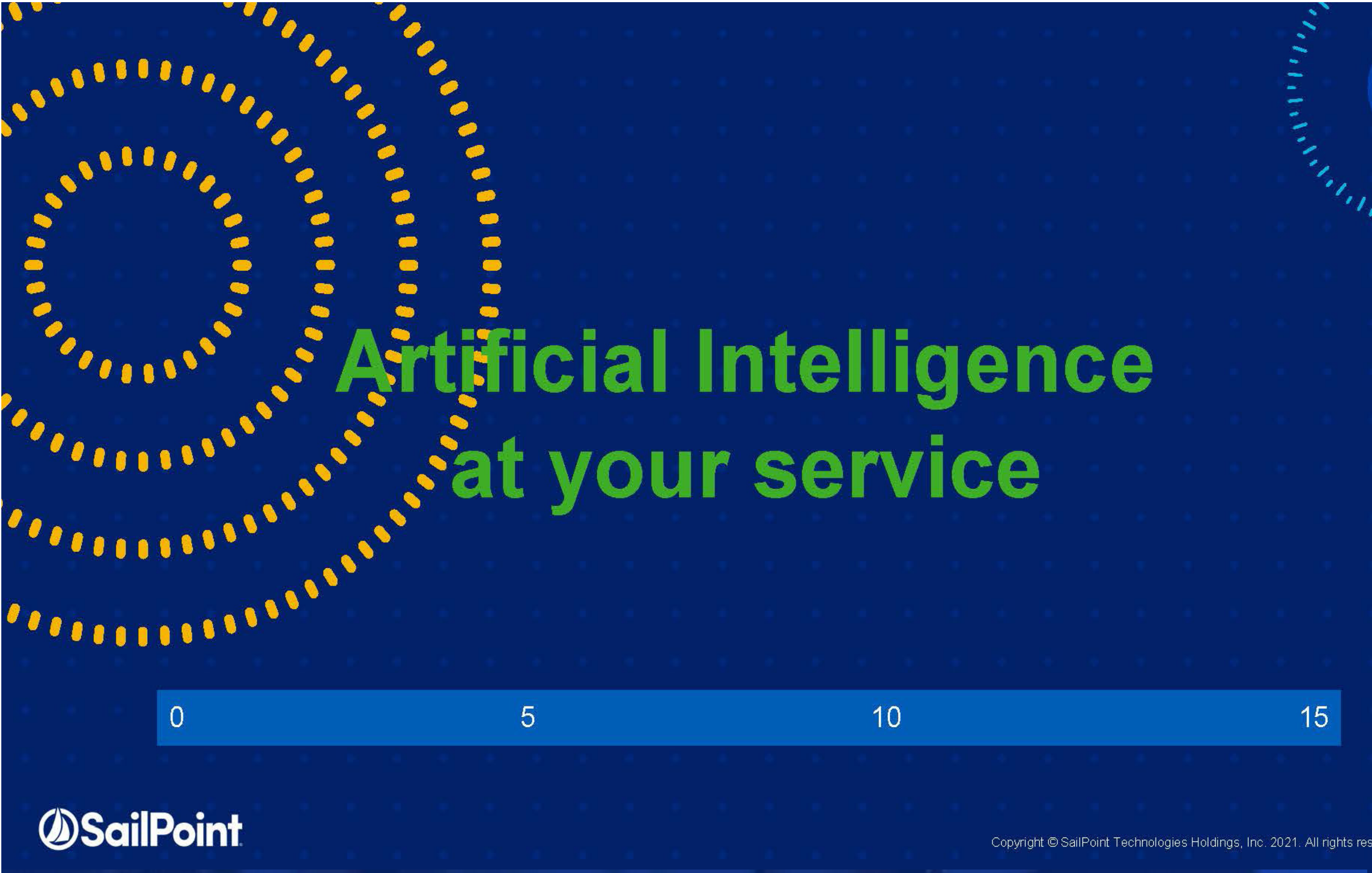
Artificial Intelligence by SailPoint

Cloud Access Management

Access Recommendations

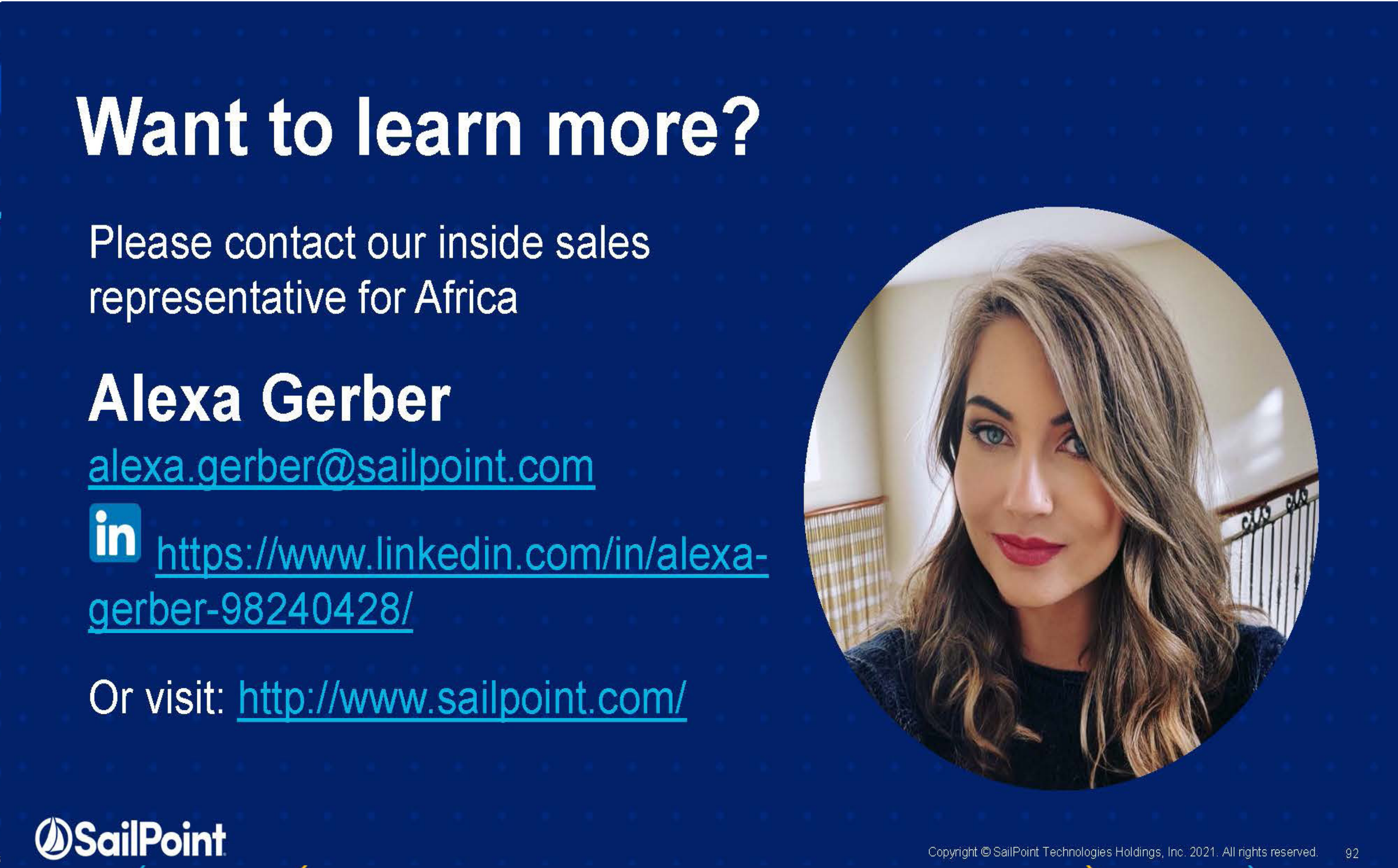
Access Modelling

Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved. 87



Artificial Intelligence at your service

Poll



Want to learn more?

Please contact our inside sales representative for Africa

Alexa Gerber

alexa.gerber@sailpoint.com

in https://www.linkedin.com/in/alexa-gerber-98240428/

Or visit: http://www.sailpoint.com/

SailPoint

92

SailPoint

Thank You

CISO Alliances

CISSOP

PROCEDURES BY PROFESSIONALS
SECURING THE BUSINESS

CISSOP by the CISO Alliances

Cyber and Information Security Standard Operating Procedures

Simply put, this has been launched to empower the end user executive to have input and control a truly end user only procedure around the true focuses in securing the business from a Cyber and Information Security perspective.

Why we are working on it?

The Cyber and Information Security Business Divisions are likely to be battling the same or similar threat landscape and impactful and disruptive breach attempts. Not much is standardised or end-user produced in terms of procedures. This is fundamentally why CISSOP by the CISO Alliances was born.

Planned Outcomes

Leverage CISO Alliances community experiences to create a standardised approach to business in Cyber and Information Security where possible

Published to the active global community

Published as a playbook. Printed and distributed to the wider Cyber and Information Security Community

Expressions of interest to be sent to

cissops@alliances.global

Can you suggest and contribute to create a standardised operating procedure with your peer?

Produced by:
ALLIANCE Media Group

Alliances Activities

CISO Alliances

UK & Ireland
Dublin
Edinburgh
Manchester
London

Executive Business Exchange

North America

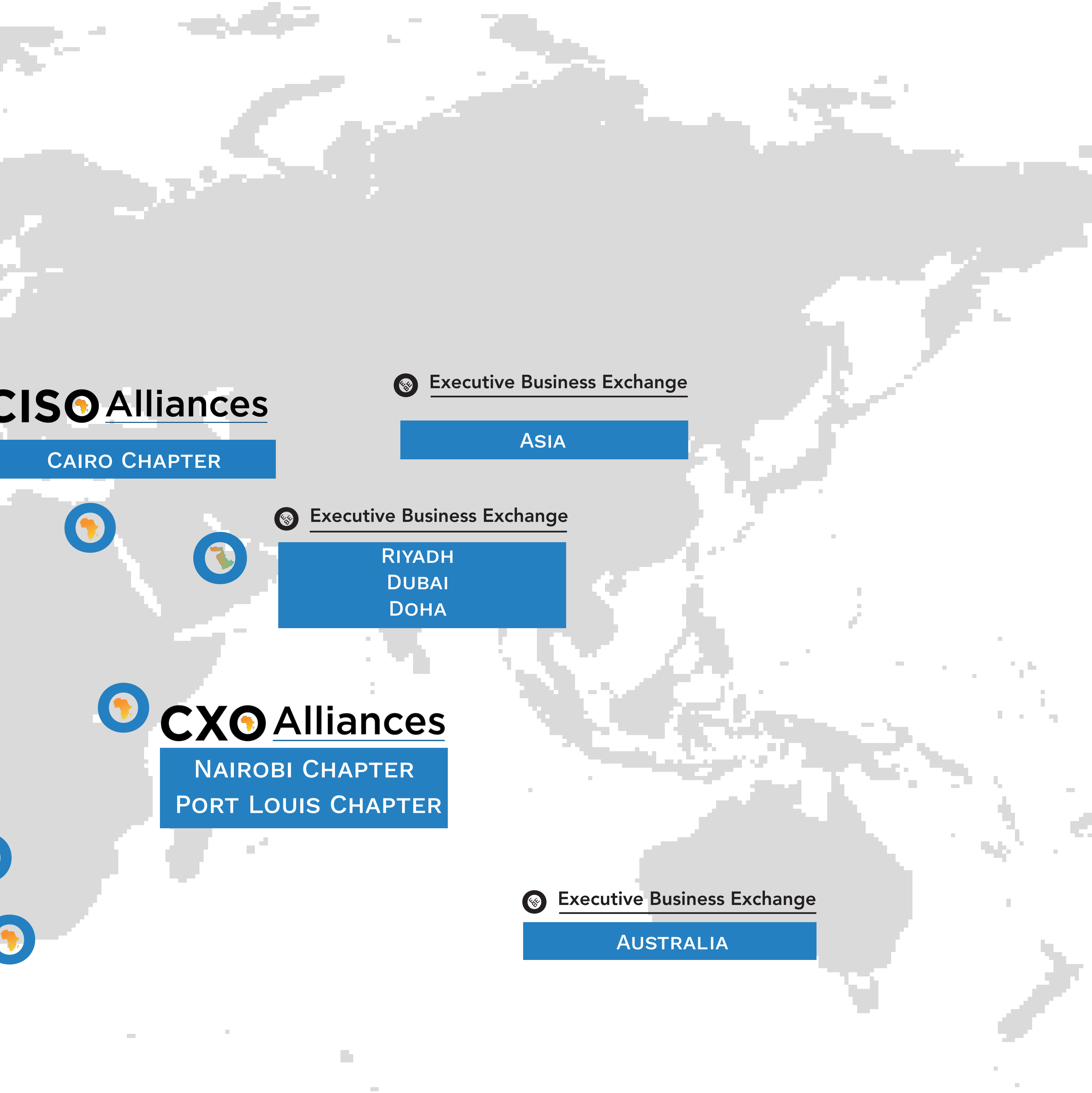
CISO Alliances

Lagos Chapter
Accra Chapter
Abuja Chapter

Executive Business Exchange

South America

CXO Alliances



CISO Alliances

Cairo Chapter

Executive Business Exchange

Asia

Executive Business Exchange

Riyadh
Dubai
Doha

CXO Alliances

Nairobi Chapter
Port Louis Chapter

Executive Business Exchange

Australia