DigitalAlliances
continue collaboration

CISO Alliances

SOUTH AFRICA CHAPTER

12TH of May 2022

Results

BeyondTrust

DigitalAlliances
continue collaboration

CISO Alliances

ALLIANCE Media Group

Alliance - 'A union formed for mutual benefit'

Community – '1: a unified body of individuals: such as. A: the people with common interests living in a particular area broadly: the area itself the problems of a large community'

DigitalAlliances
continue collaboration

Executive Business Exchange

DPO Alliances

CIO Alliances

CISO Alliances

CXO Alliances

CMO Alliances

CDO Alliances

CISO Alliances

ALLIANCE Media Group

Foreword

Leigh Thomas
Director & Founder

We are a group of driven and ambitious professionals who strive to achieve the ideal.

We have built and participated in C-level communities in a variety of industries, including Oil & Gas, Mining, Power & Enterprise IT, Information and Cyber Security, and across many divisions.

The Alliances Community's basic ideals were born along with Alliance Media Group, as defined by the Collins dictionary: "A union formed for mutual benefit." Everyone must believe in their own ability to succeed and improve. This can only be accomplished via selflessness in sharing and genuine feedback from everyone to whom we devote our time.

We no longer consider this industry to be B2B, but rather P2P. (Peer to Peer). Our intentions are to create a trusted platform for executives tackling similar business objectives to leverage their collective experience to support one another, debate opinions candidly for industry progression and professional growth, and benchmark strategies against one another, which we have been doing since August 2016. This is the community for CISO Alliances. The community built it for the community.

While understanding that in order to be sustainable in the modern world, every business will need to drive commercials. We believe that commercials should not be the driving force, but rather a solution to a 'why'.

Our Chapters and community are working to make an impact on the Events Managed Services industry, which continues to act as if money is the most important factor and not the value of time. The industry was founded on the premise that "everyone wants to learn," and we established the Alliances to ensure that end-user-driven meetings are solely focused on the educational needs of everyone involved as well as their business objectives. Focusing on the best practises for overcoming the common business objectives that motivate activity within each end user firm, rather than just global trends and themes to generate revenue.

Due to the Coronavirus pandemic, the digital environment has been forced to accommodate a remote workforce with limited human interaction since March 2020. As a result, our community representative has been open to digital chapters in addition to physical chapters when they return in Q3 2022. This complements our efforts in community building and makes the community feel like they are part of a continuous effort to meet their educational needs.

11.45

Welcome Remarks & Joining Time

12.05

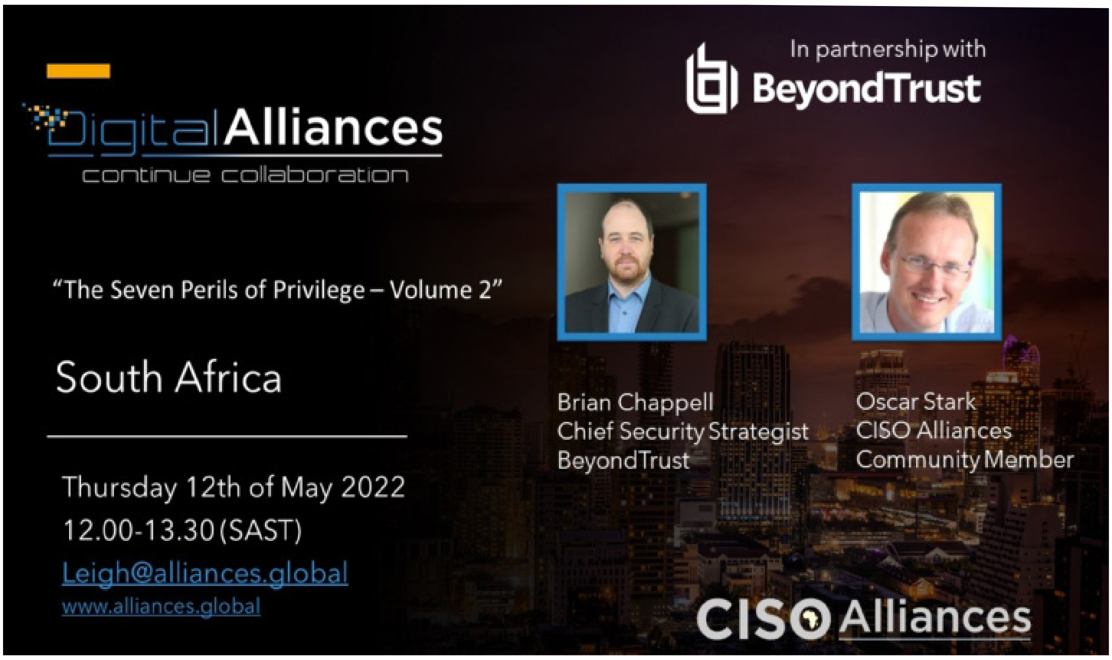
Overview

Session Leaders:

Brian Chappell, Chief Security Strategist – BeyondTrust
Oscar Stark, CISO Alliances Community Member

Session Title:

The Seven Perils of Privilege – Volume 2



DigitalAlliances
continue collaboration

In partnership with
BeyondTrust

"The Seven Perils of Privilege – Volume 2"

South Africa

Thursday 12th of May 2022
12.00-13.30 (SAST)
Leigh@alliances.global
www.alliances.global

Brian Chappell
Chief Security Strategist
BeyondTrust

Oscar Stark
CISO Alliances
Community Member

CISO Alliances

12.50

Q & A

13.25

Action Areas and Next Steps

DigitalAlliances
continue collaboration

CISO Alliances

Overview

Date: Thursday, 12th of May 2022

Time: 12.00 pm – 13.30 pm (SAST)

Platform: Digital Alliances

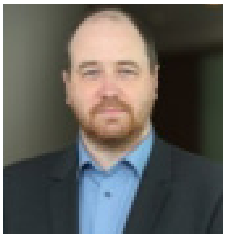
Location: Digital Alliances – Microsoft Teams Link – Invite Only

Overall Theme: **The Seven Perils of Privilege – Volume 2**

The Digital Alliances is a platform created to ensure our communities are enabled to utilise our candid approach to benchmark and to continue collaboration where physical Chapters are restricted

BeyondTrust

Focused Session



Session Leaders

Brian Chappell, Chief Security Strategist – BeyondTrust

Oscar Stark, CISO Alliances Community Member

The Seven Perils of Privilege – Volume 2

For those who attended our first session on The Seven Perils of Privilege in 2021, you should remember that it was so vocal and interactive that we didn't actually have the chance to reach our Peril #2... and that is a good problem to have. It means that the topic is of interest and that privilege management is more than ever a sensitive and yet critical challenge to tackle.

And so we're back with our Seven Perils of Privilege. For this Volume 2, we will address what these perils are, their causes, the effects of leaving them unaddressed, and (most importantly) solutions. But we will have a particular focus on how the Zero Trust approach and the proliferation of ransomware may have impacted your overall cybersecurity strategy.

So join us to learn and brainstorm:

- What the seven perils of privilege are and which ones represent the highest risks for your peers
- Why poor password practices, lax cloud security (and much more) create risk
- How can organizations reduce some of these risks

Ready to take control of privileges? Join us to learn more and leave with key practical takeaways.

DigitalAlliances continue collaboration

CISO Alliances

Takeaways

What do you think of the cybersecurity model that make use of COBIT or NIST with CIS/CSF benchmark?

There are so many common aspects of regulatory compliances that make almost all applicable when looking at a cybersecurity strategy, particularly if you are struggling with where to start. Zero Trust, like so many cybersecurity models, builds on from other approaches – at least in regard to the cybersecurity basics which are so essential in ensuring our security operation is built on solid foundations.

To put the board at ease, what security dashboard would you recommend? What what should be included on the dashboard?

Dashboards are going to be largely individual and driven by your Board. That said, remember that the Board are focused on organisational success which is often dominated by risk. Being able to present the cybersecurity status in terms of organisational risk will give you the most direct route to both their attention and understanding. Review the dashboard with your Board, check they understand what's presented and that the information is valuable to them. Like any metrics, focus on the information that is important and relevant to the audience and are going to support your activity. This doesn't mean hiding data but rather ensuring that everything presented has value and informs.

Have you identified larger organisations that are already operating at an optimal zero trust maturity level?

Zero Trust as an approach is still relatively early in terms of adoption for many organisations and the progress along the journey varies from business to business. I'm not aware of any organisation that has reached a 'maintain' state ('maintain state' = the underlying infrastructure, technology, processes and people are in place and they are now tracking developments to expand and improve their ZT architecture) in their Zero Trust efforts. Many organisations are concerned that they are behind the curve in cybersecurity journey but I would suggest that they are definitely not alone. The only truly bad cybersecurity implementation is the one that hasn't started yet.

Takeaways

Assessing security on cloud platforms, especially aaS applications is easier said than done. Just knowing what questions to ask and what to check is a challenge

While the Cloud has been around for many years now, the form has evolved and the capabilities have mushroomed. Don't be afraid to ask Cloud Service Providers what other organisations are asking them for but make sure anything you take into your list are requirements for your business. This is the biggest stumbling block I see for any cybersecurity project, or in fact any project. Poor requirements gathering will impact your efforts making it ever harder to reach any kind of maturity. Ensure everything on the requirements list links back to a business benefit (tangible or intangible) and your questions will then be around how the CSP delivers against those requirements.

With cloud adoption, we see more and more use of APIs, naturally. Any thoughts on API security and related UAM/PAM?

APIs present a challenge as, in many ways, as we need to secure them but they are often also high volume services that have data integrity requirements. Positioning something between your app and the API(s) it's using could have negative impacts both on performance and integrity. That said, API gateways offer great opportunity to abstract both the APIs and the access to them into a far more granular approach.

How should you handle credentials in a devsecops environment?

Carefully. DevOps and DevSecOps tend to be highly automated environments (lots of scripts) that operate at high transaction volumes. It's essential that we build or adapt those environments to leverage solid PAM principles and tools sooner rather than later – the size of the problem space is growing rapidly and beyond linearly. DevOps tools already exist to manage the credentials in these environments. Tools built on the same technologies are the DevOps/DevSecOps systems with the same elastic scaling and resilience those environments need.

Takeaways

Password renewal with set days until change question/ MFA?

The death of passwords has been declared dozens of times over recent years and they are still here. What has changed is what the primary authentication mechanism is. We see increasing use of biometrics for human-machine authentication and the rise of MFA (usually just 2 factors – password and token) where, in truth, the token is the primary authentication mechanism despite it being the second entered. Passwords will remain as a fallback even when auth is biometric and/or token. For machine-to-machine authentication (or system-to-system), the password will endure because it has to. In the term password I include any string of characters or bytes presented as an authentication token. Machines/applications don't have eyes, faces, fingerprints, etc. and necessarily need to contain everything needed to authenticate within their 'box'. This is where Zero Trust, with its segmented trust zones, can really shine. If you ensure all access to a restricted resources comes from trusted IP addresses (app servers and PAM session proxies) then you contain the scope of the passwords. There are other layers of security to apply but there are some big wins to be made with relatively simple technology and a consistent approach.

Telco regulator (ICASA) has placed the burden on telcos to capture fingerprints of customers. This will make Telco the target for hackers. Not only that if they bridge the systems where we store the fingerprint scans it carte-blanche.

Any organisation that stores sensitive personally identifiable information (PII) will naturally be a target for hackers but we already have guidance on how to address the storage and management of such information. There are number of data privacy regulations across the world to draw upon (even if your country doesn't have one yet – it will and it'll necessarily be based on existing legislation) and Zero Trust will definitely contribute significantly to that kind of security by promoting smaller trust zones and segmentation limiting access to the stored fingerprints to only those systems and services that absolutely need it.

BeyondTrust

DigitalAlliances
continue collaboration

CISO Alliances

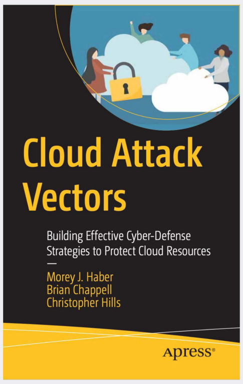
BeyondTrust

Zero Trust

Getting Least Privilege Right, Finally

Brian Chappell
Chief Security Strategist

- 30+ years IT and cybersecurity experience
- Senior roles in vendors, OEMs, system integrators, and multi-nationals in Support, Software Development, Product Management, Project Management, Architecture, Operations and Sales Engineering
- Co-author of the upcoming book Cloud Attack Vectors published by Apress (Available 21st July 2022)


Cloud Attack Vectors

Building Effective Cyber-Defense Strategies to Protect Cloud Resources

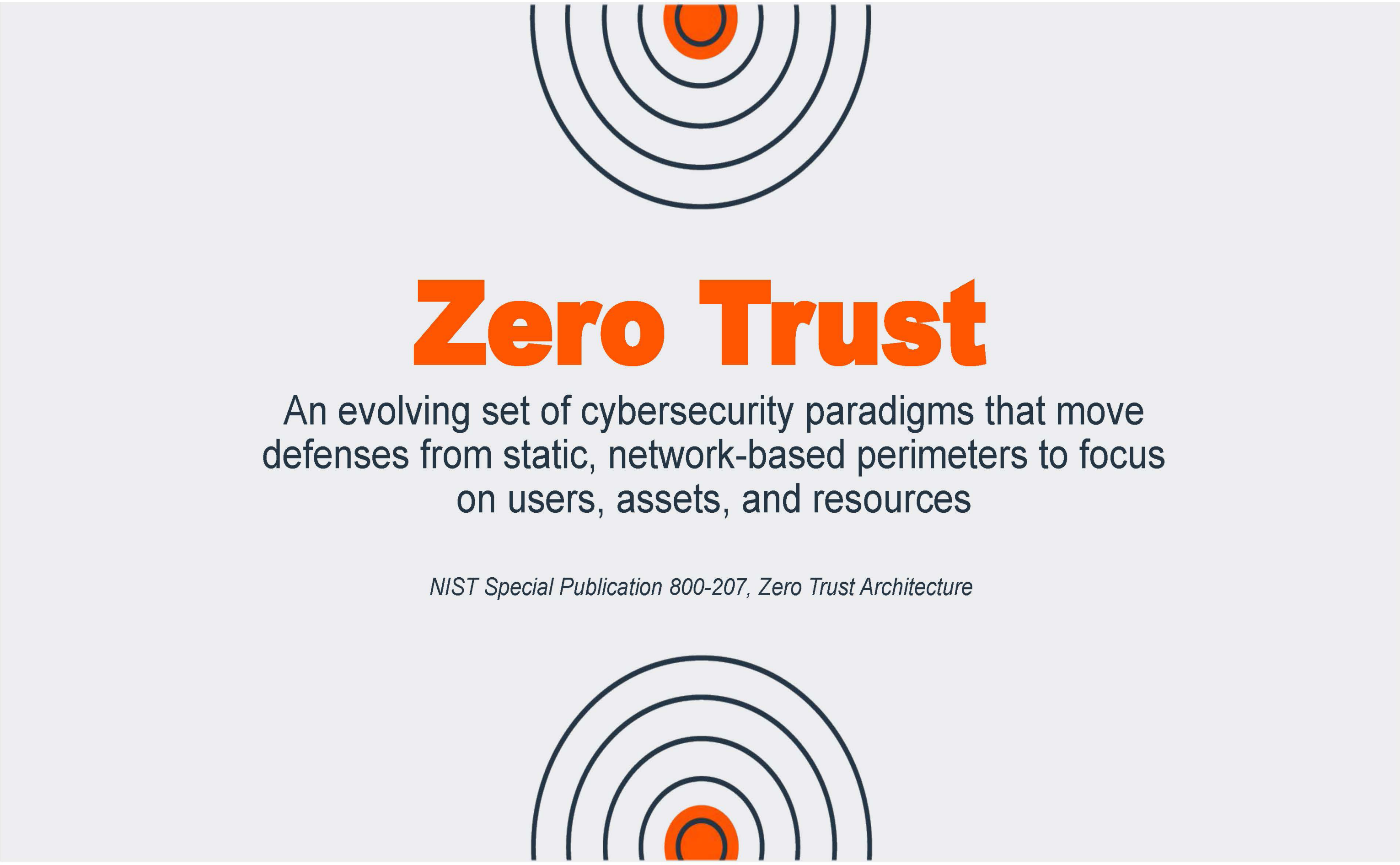
Morey J. Haber
Brian Chappell
Christopher Hills

Apress

The Zero Trust framework is still fairly vague in terms of what specific technology is required, and how to implement it.

Consequently, it has become an industry buzzword that can mean many different things.

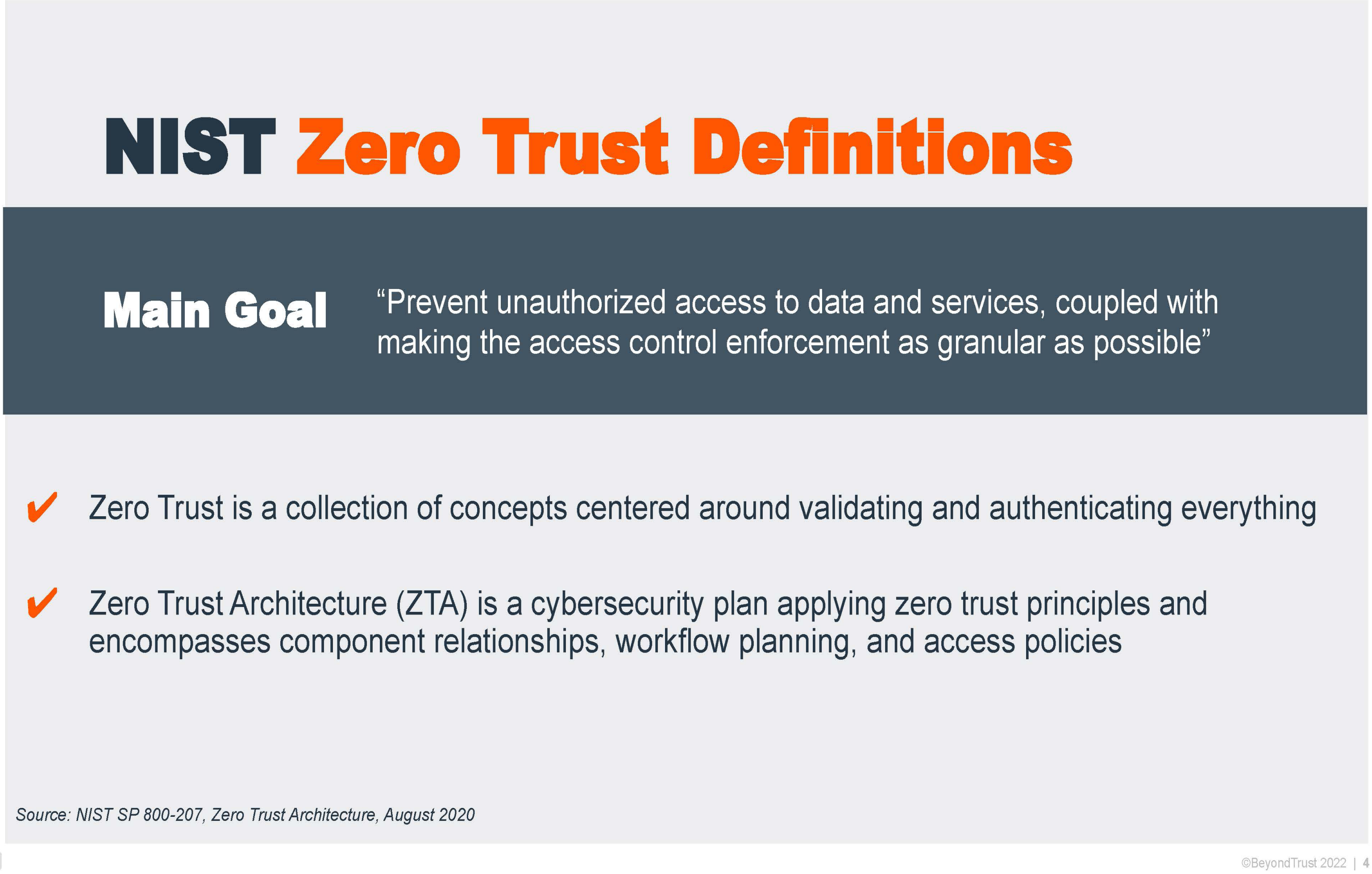
InfoSecurity Magazine
Feb 10, 2021



Zero Trust

An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources

NIST Special Publication 800-207, Zero Trust Architecture

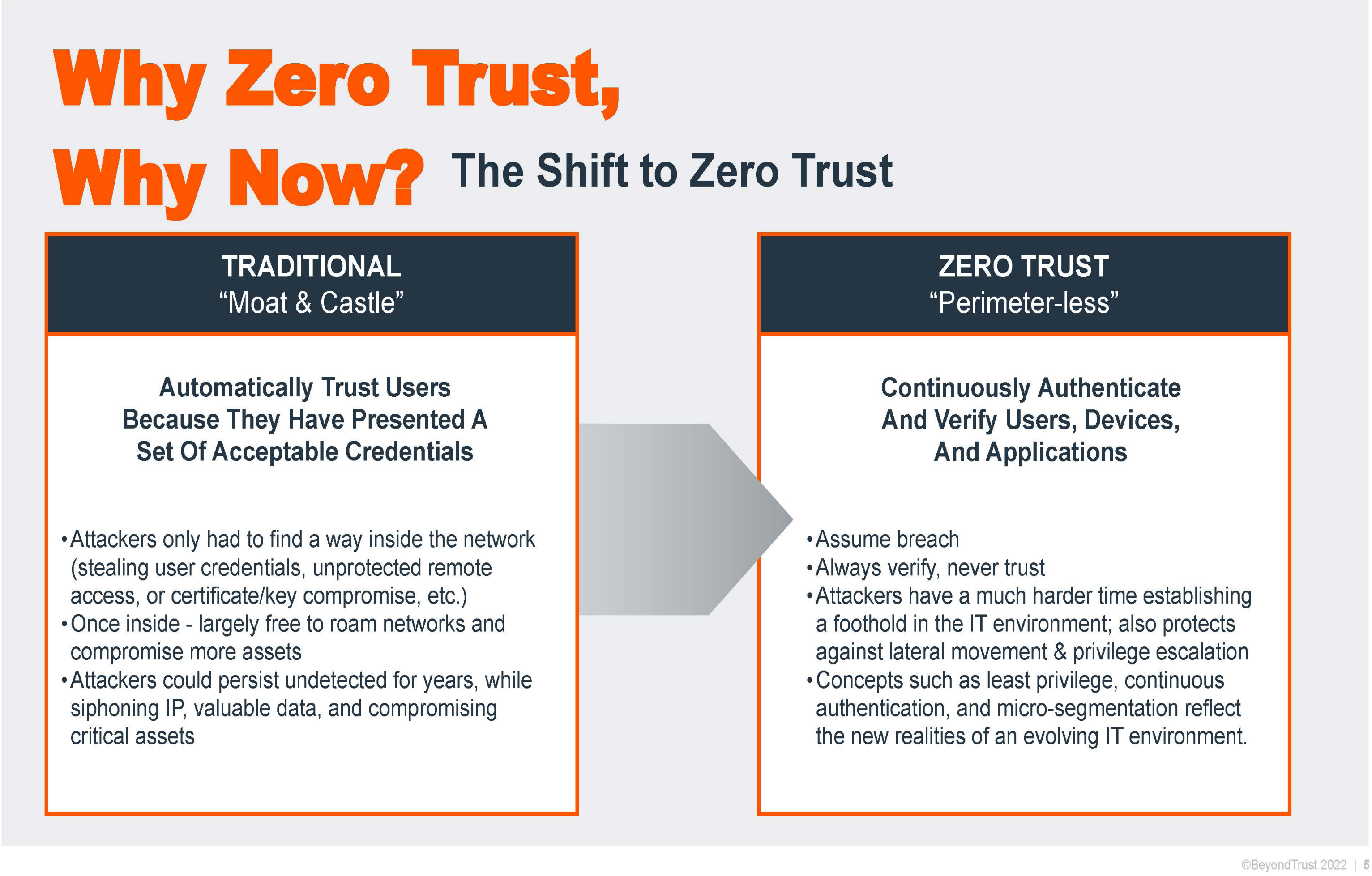


NIST Zero Trust Definitions

Main Goal “Prevent unauthorized access to data and services, coupled with making the access control enforcement as granular as possible”

- ✓ Zero Trust is a collection of concepts centered around validating and authenticating everything
- ✓ Zero Trust Architecture (ZTA) is a cybersecurity plan applying zero trust principles and encompasses component relationships, workflow planning, and access policies

Source: NIST SP 800-207, Zero Trust Architecture, August 2020



Why Zero Trust, Why Now?

The Shift to Zero Trust

TRADITIONAL
“Moat & Castle”

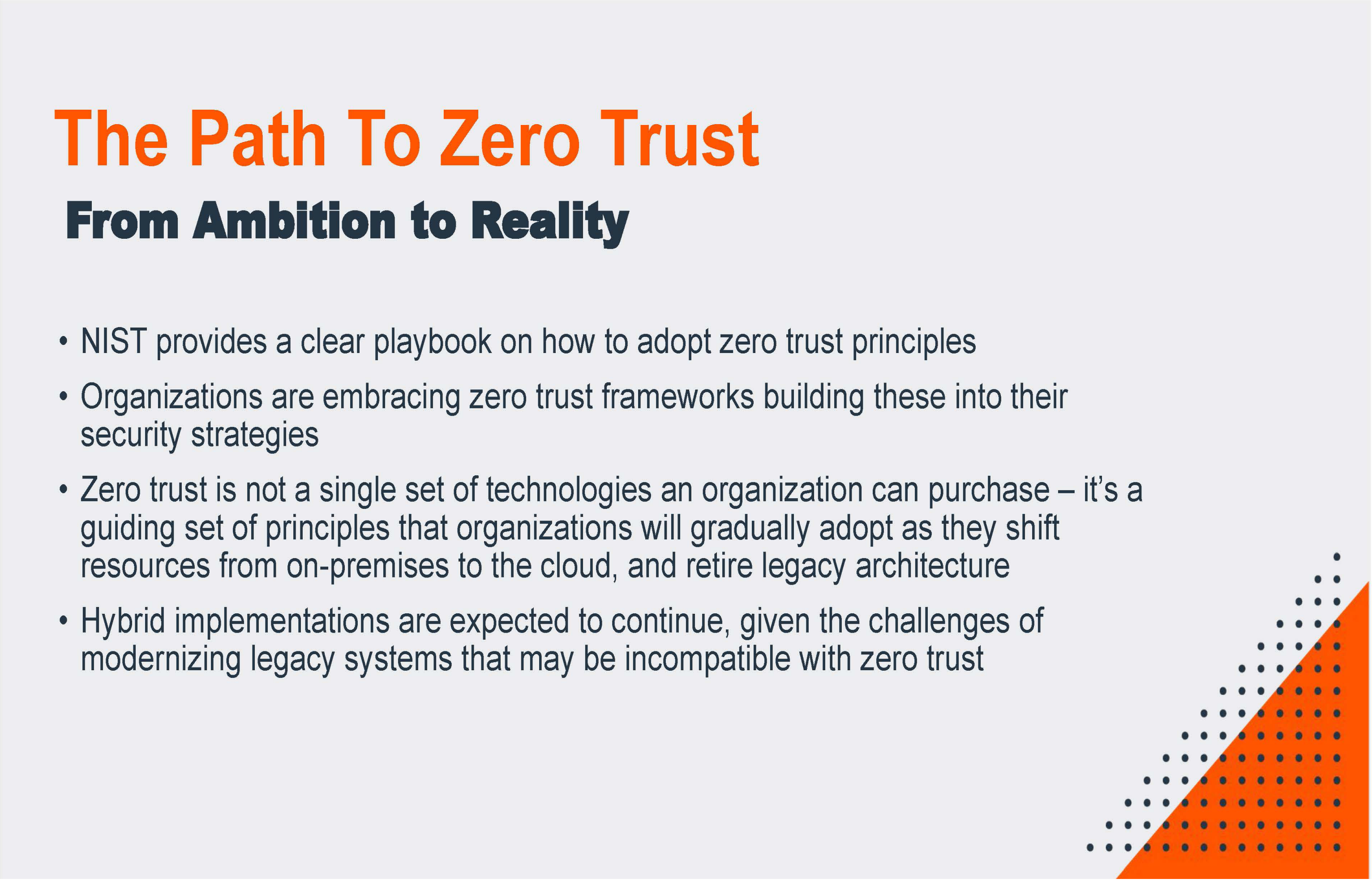
Automatically Trust Users Because They Have Presented A Set Of Acceptable Credentials

- Attackers only had to find a way inside the network (stealing user credentials, unprotected remote access, or certificate/key compromise, etc.)
- Once inside - largely free to roam networks and compromise more assets
- Attackers could persist undetected for years, while siphoning IP, valuable data, and compromising critical assets

ZERO TRUST
“Perimeter-less”

Continuously Authenticate And Verify Users, Devices, And Applications

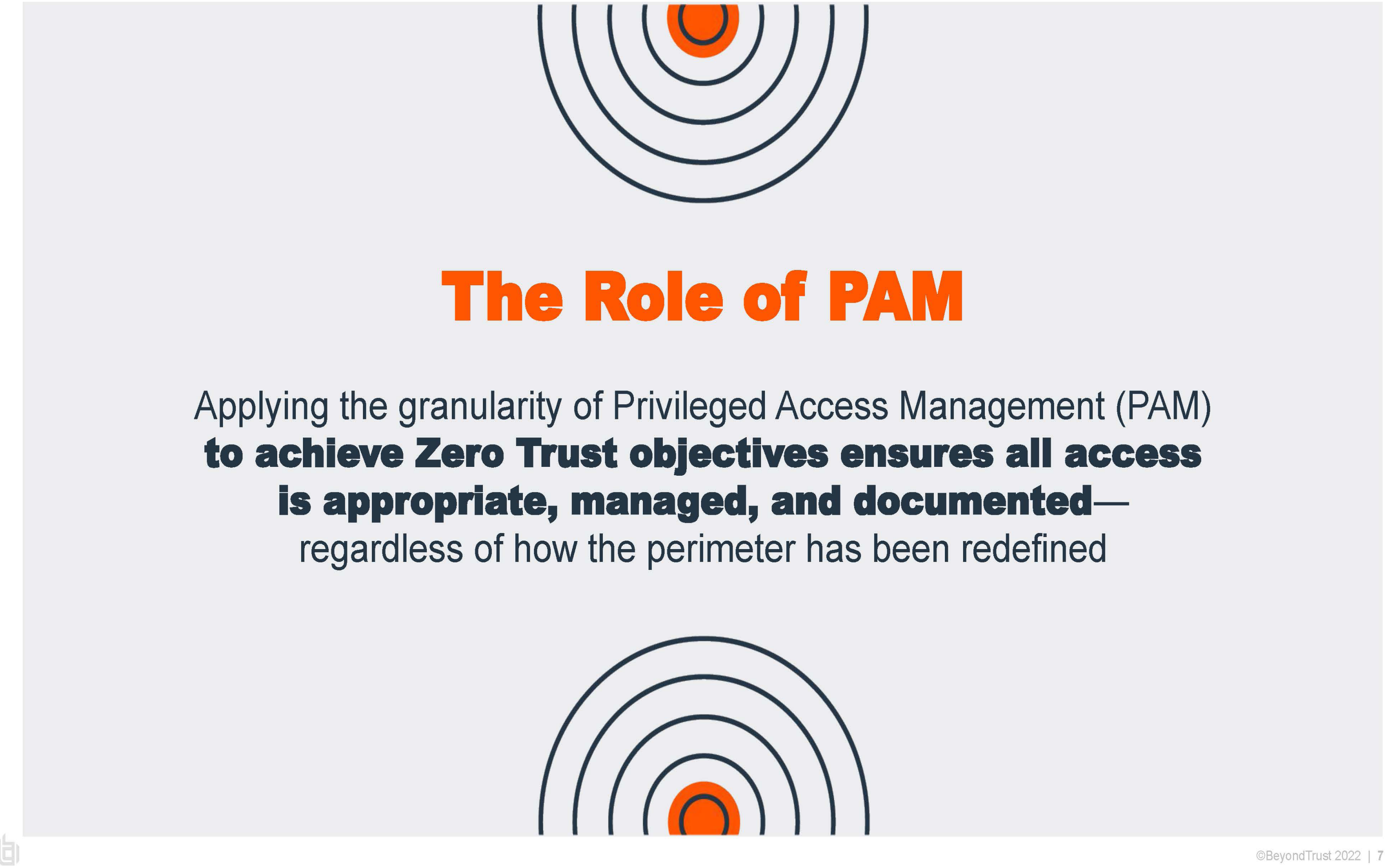
- Assume breach
- Always verify, never trust
- Attackers have a much harder time establishing a foothold in the IT environment; also protects against lateral movement & privilege escalation
- Concepts such as least privilege, continuous authentication, and micro-segmentation reflect the new realities of an evolving IT environment.



The Path To Zero Trust

From Ambition to Reality

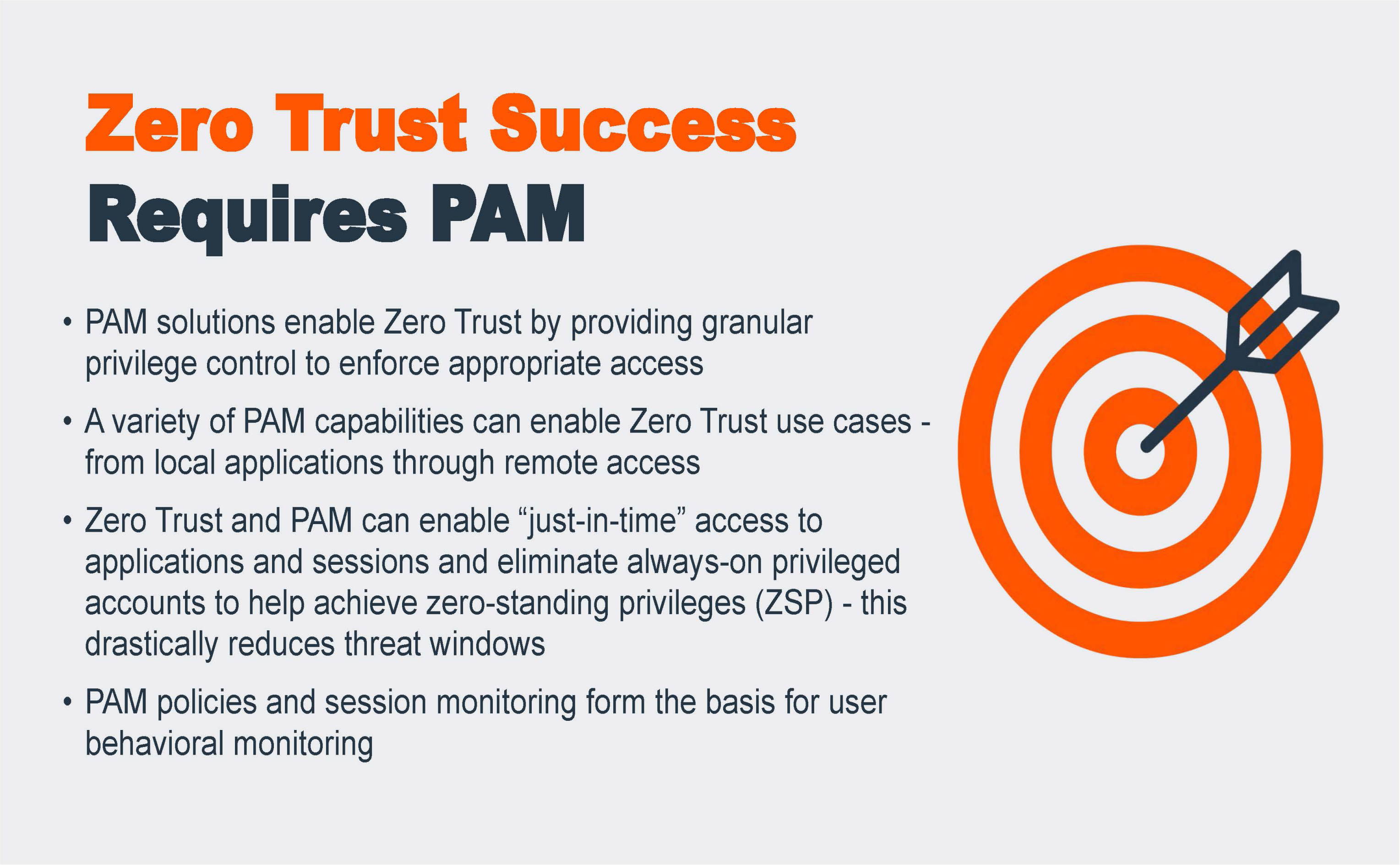
- NIST provides a clear playbook on how to adopt zero trust principles
- Organizations are embracing zero trust frameworks building these into their security strategies
- Zero trust is not a single set of technologies an organization can purchase – it's a guiding set of principles that organizations will gradually adopt as they shift resources from on-premises to the cloud, and retire legacy architecture
- Hybrid implementations are expected to continue, given the challenges of modernizing legacy systems that may be incompatible with zero trust



The Role of PAM

Applying the granularity of Privileged Access Management (PAM) **to achieve Zero Trust objectives ensures all access is appropriate, managed, and documented**— regardless of how the perimeter has been redefined

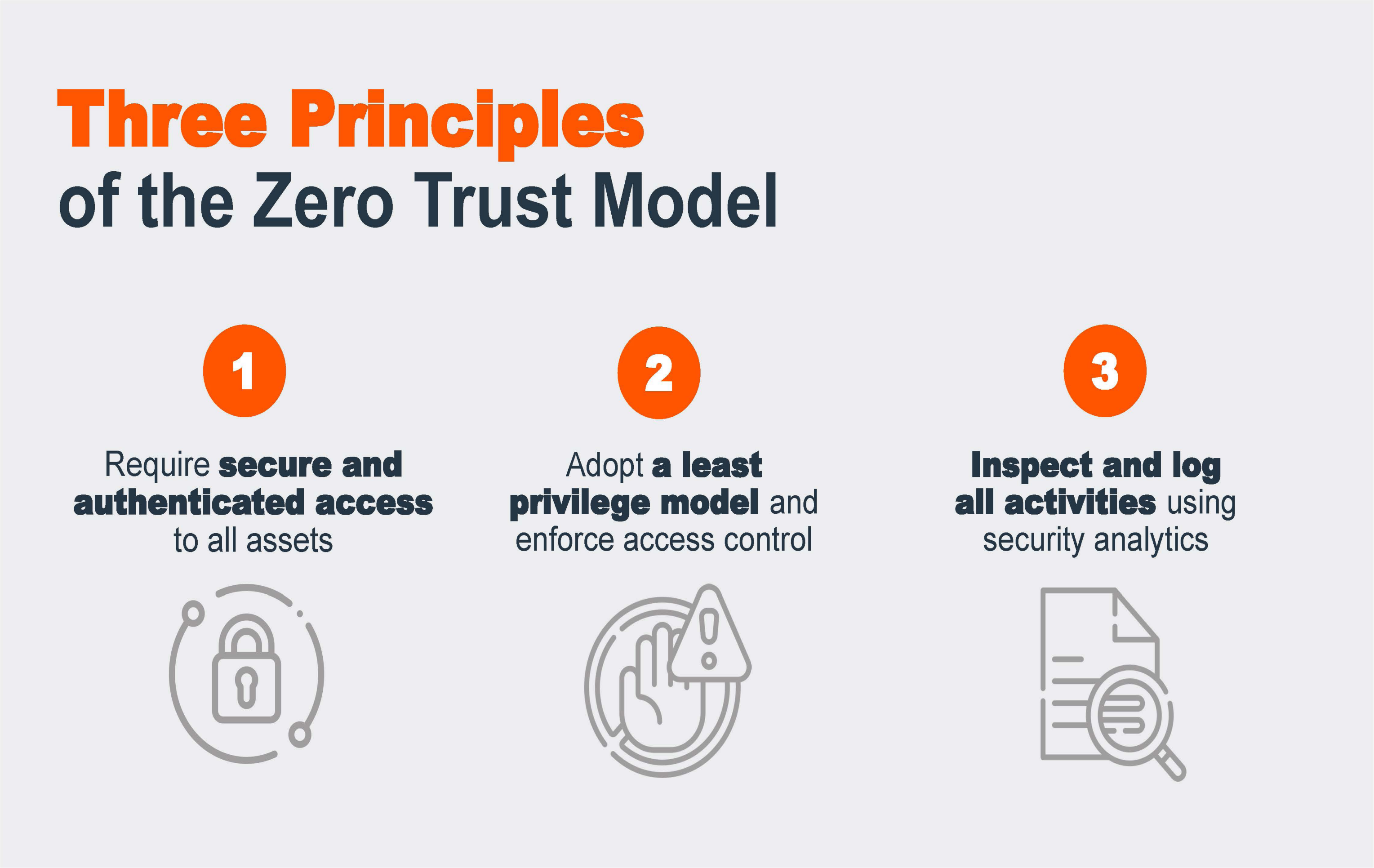
©BeyondTrust 2022 | 7



Zero Trust Success Requires PAM

- PAM solutions enable Zero Trust by providing granular privilege control to enforce appropriate access
- A variety of PAM capabilities can enable Zero Trust use cases - from local applications through remote access
- Zero Trust and PAM can enable “just-in-time” access to applications and sessions and eliminate always-on privileged accounts to help achieve zero-standing privileges (ZSP) - this drastically reduces threat windows
- PAM policies and session monitoring form the basis for user behavioral monitoring

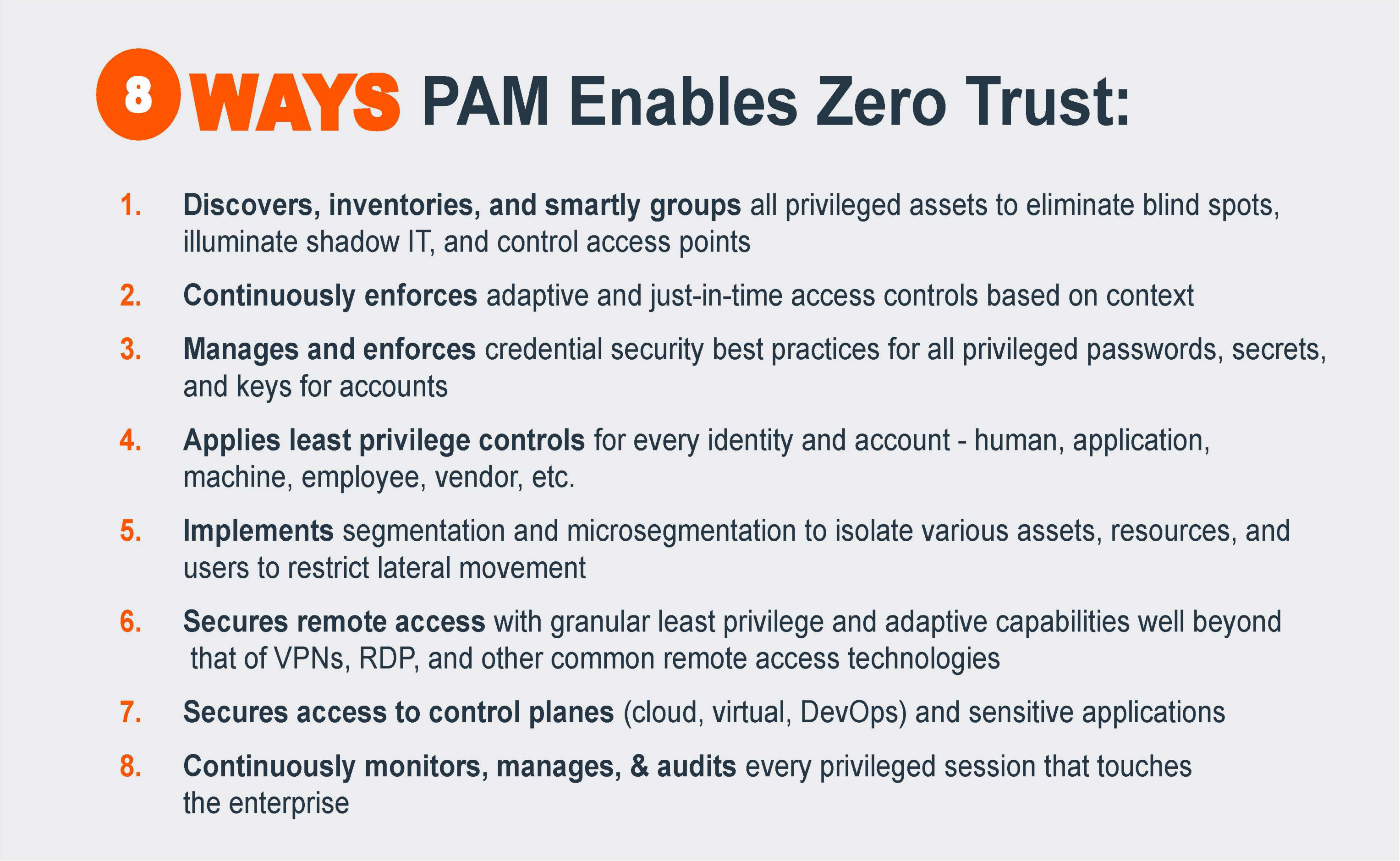
©BeyondTrust 2021 I 8



Three Principles of the Zero Trust Model

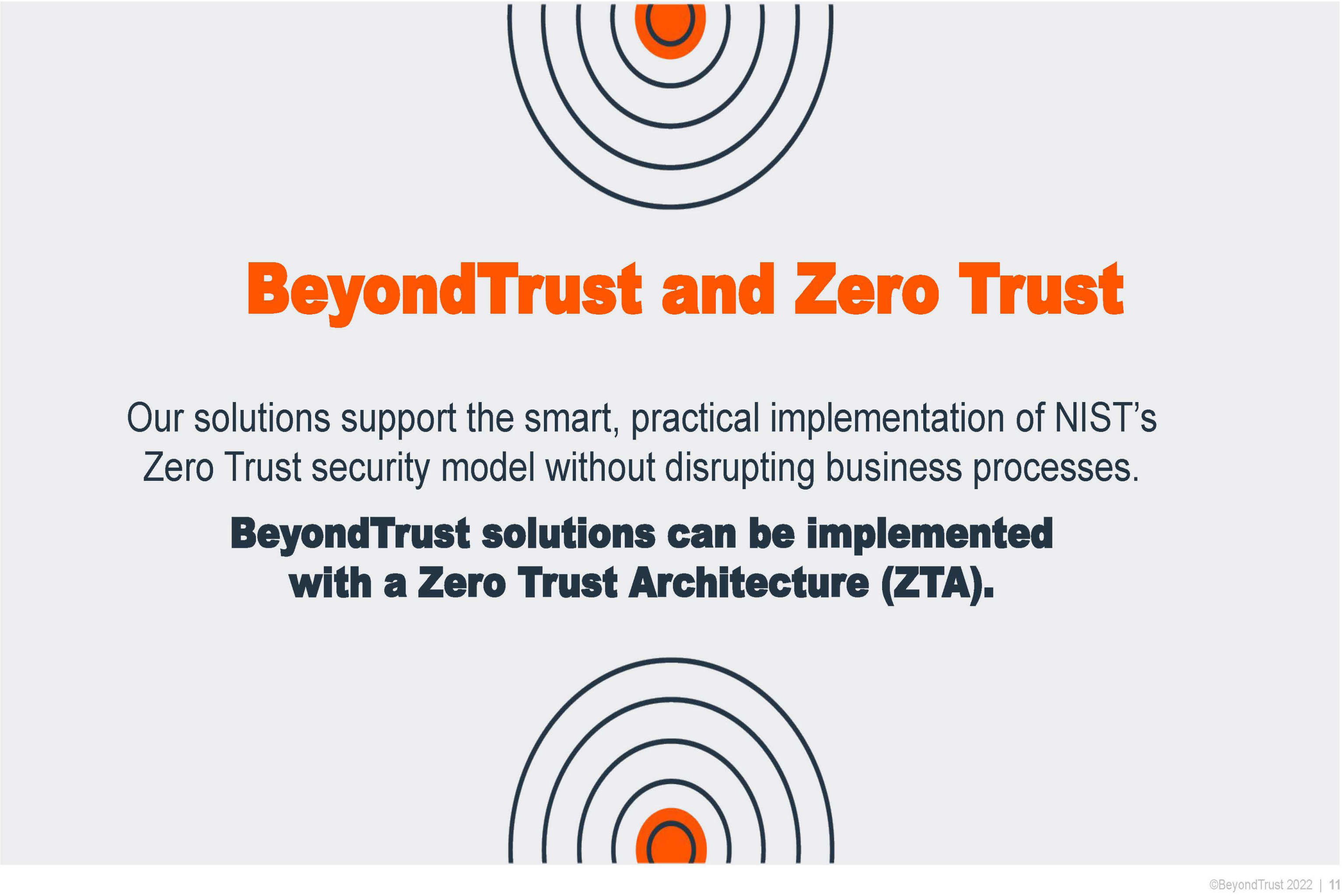
1. Require **secure and authenticated access** to all assets
2. Adopt **a least privilege model** and enforce access control
3. **Inspect and log all activities** using security analytics

©BeyondTrust 2022 | 9



8 WAYS PAM Enables Zero Trust:

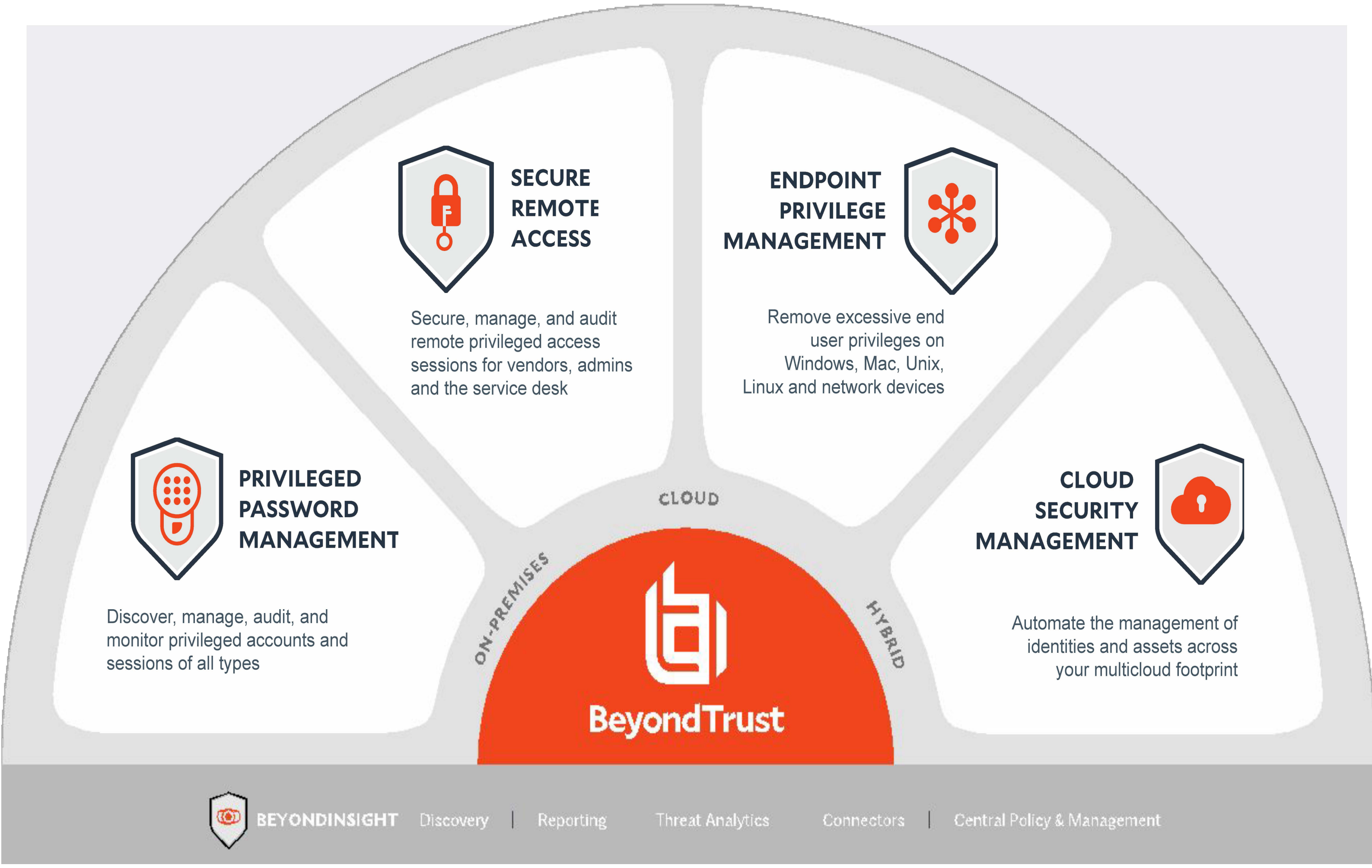
1. **Discovers, inventories, and smartly groups** all privileged assets to eliminate blind spots, illuminate shadow IT, and control access points
2. **Continuously enforces** adaptive and just-in-time access controls based on context
3. **Manages and enforces** credential security best practices for all privileged passwords, secrets, and keys for accounts
4. **Applies least privilege controls** for every identity and account - human, application, machine, employee, vendor, etc.
5. **Implements** segmentation and microsegmentation to isolate various assets, resources, and users to restrict lateral movement
6. **Secures remote access** with granular least privilege and adaptive capabilities well beyond that of VPNs, RDP, and other common remote access technologies
7. **Secures access to control planes** (cloud, virtual, DevOps) and sensitive applications
8. **Continuously monitors, manages, & audits** every privileged session that touches the enterprise



BeyondTrust and Zero Trust

Our solutions support the smart, practical implementation of NIST's Zero Trust security model without disrupting business processes.

BeyondTrust solutions can be implemented with a Zero Trust Architecture (ZTA).



SECURE REMOTE ACCESS

Secure, manage, and audit remote privileged access sessions for vendors, admins and the service desk

ENDPOINT PRIVILEGE MANAGEMENT

Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices

PRIVILEGED PASSWORD MANAGEMENT

Discover, manage, audit, and monitor privileged accounts and sessions of all types

CLOUD SECURITY MANAGEMENT

Automate the management of identities and assets across your multicloud footprint

BEYONDINSIGHT Discovery | Reporting Threat Analytics Connectors | Central Policy & Management

BeyondTrust Resources

A ZERO TRUST APPROACH TO SECURE REMOTE ACCESS

Protecting Privileged Access for All Remote Sessions

ZERO TRUST PPROACH TO VINDOWS & MAC NDPOINT SECURITY

ieving a Zero Trust Architecture with point Privilege Management

Zero Trust Approach Privileged Password Management

curing Resources From Inappropriate Access

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

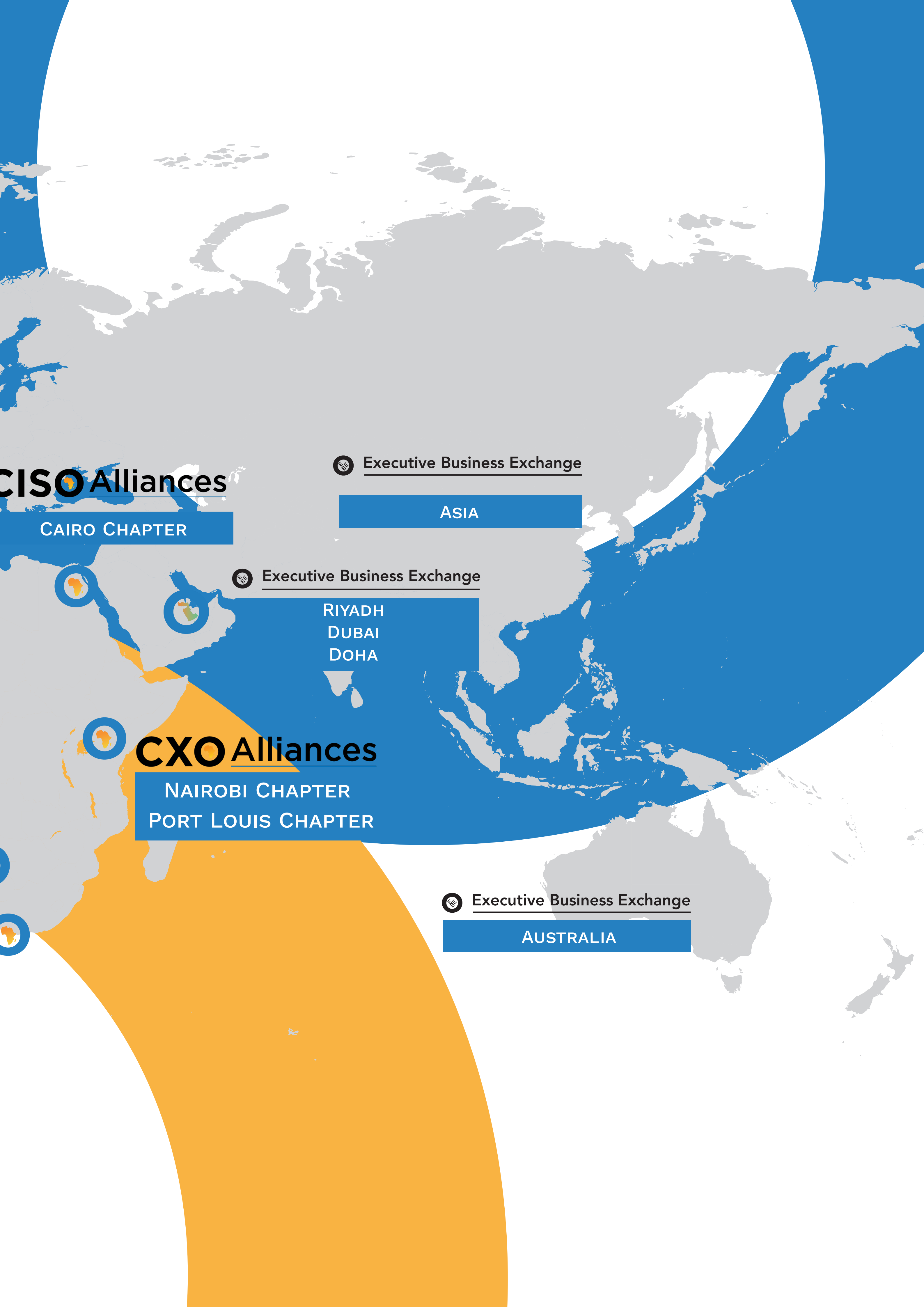
Lagos Chapter
Accra Chapter
Abuja Chapter

Executive Business Exchange

South America

CXO Alliances

Western Cape Chapter
KwaZulu Natal Chapter
Gauteng Chapter



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