CISO Alliances

Digital Alliances Session

13th October 2022

Results

Digital Alliances
continue collaboration

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’

Foreword

Leigh Thomas
Director & Founder

We are a team of ambitious and passionate executives with a desire for achieving the ideal.

We have experience in numerous industries in building and participating in C-level communities across the globe in Oil & Gas, Mining, Power & Enterprise IT, Info and Cyber Security, across multiple divisions across the business.

The core values of the Alliances Community were born along with Alliance Media Group appropriately put by the Collins dictionary definition - Alliance - 'A union formed for mutual benefit'. Everyone must feel like there is success and progression. This is only achieved with selflessness in sharing and candid feedback from all that we commit our time to.

We, as a group, no longer view this industry as B2B but P2P (Person to Person). Our intentions are to, and since August 2016 have been to create a trusted platform for people who are executives combating similar business objectives to leverage their collective experience to help one and other, debate opinions candidly for industry progression and professional growth and to benchmark strategies against one and other. This is the CISO Alliances community. Built by the community for the community.

Whilst understanding that every business will need to drive commercials to become sustainable in the modern world. We believe 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 where ego is the drive and industry professional growth. The industry was born off the back of 'Everybody wants to learn' and we 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. With every hope that we can safely run physical chapters as soon as possible.

Overview

Date: Thursday, 13th October 2022

Time: 9:00am – 10:30am (SAST)

Venue: Invite only by Regional Director – Microsoft Teams

The Alliances chapter is a gathering consists of business risk, information and cyber security leaders who have been highlighted as being able to offer value in terms of content and influence. It is designed to form alliances and to drive progressive change in the business world and beyond.

The content and format is designed to talk together, learn better and experience more.

Format: Invite only Security and ICT Leaders debating pertinent, real life issues through the form of digital open forum.

Chatham House Rule will be applied

Outcomes:

1. Depth achieved around business objectives where the opportunity of experience within the attendees is leveraged
2. Benchmarking and verification of thought processes outside of existing networks i.e. the broader CISO Alliances community
3. Industry progression and unity in impacting the challenges of the common business objectives
4. Not corporate flag waiving or sales pitches. We insist, do that elsewhere.

Themes:

Separating the reality from the myth: The Trust or not to Trust – A Tale of Zero Trust

Workshop

09.00

Separating the reality from the myth: The Trust or not to Trust – A Tale of Zero Trust

Session Leaders: David Jackson – Lead, Cybersecurity Africa Region
Kevin Wilson – GM:IT
Nadia Veeran- Patel – Information Security Officer

Session Outcomes and Takeaways:

A community member will give us their approach to Zero Trust and what their expectations were versus their reality.

Feedback from reviewing all the different tools on the market and what has that experience been like and what am we are looking for exactly (gaps to cover).

Myths: Price points, resources and only for remote workforce.

2022 Zero Trust

How does this work?

The problem

Future	Current	Problem statement
The ideal is to not trust anything or anyone by default. The focus is on users, assets and resources to determine trust, not static based parameters.	Most systems have defaults that assume a certain level of trust for locations or assets. Replacing those systems or standards with something that assumes no trust.	Putting Zero Trust into place needs to be carefully planned as the levels of assumed trust currently keep the business running.

CISO Alliances

Digital Alliances Session

October 13th 2022

www.alliances.global

Digital Alliances
continue collaboration

Challenges deep-dive

Core → Network → Edge

Systems

The current ability to limit access is rudimentary, most systems would need to be wrapped.

Integration to many services

The current paradigm has VPN or network boundaries but allows general access to all resources. Complex firewall rule sets.

Customer experience

Limiting visibility and access increases the friction and creates an unfriendly experience for the users so adoption is low

Solution

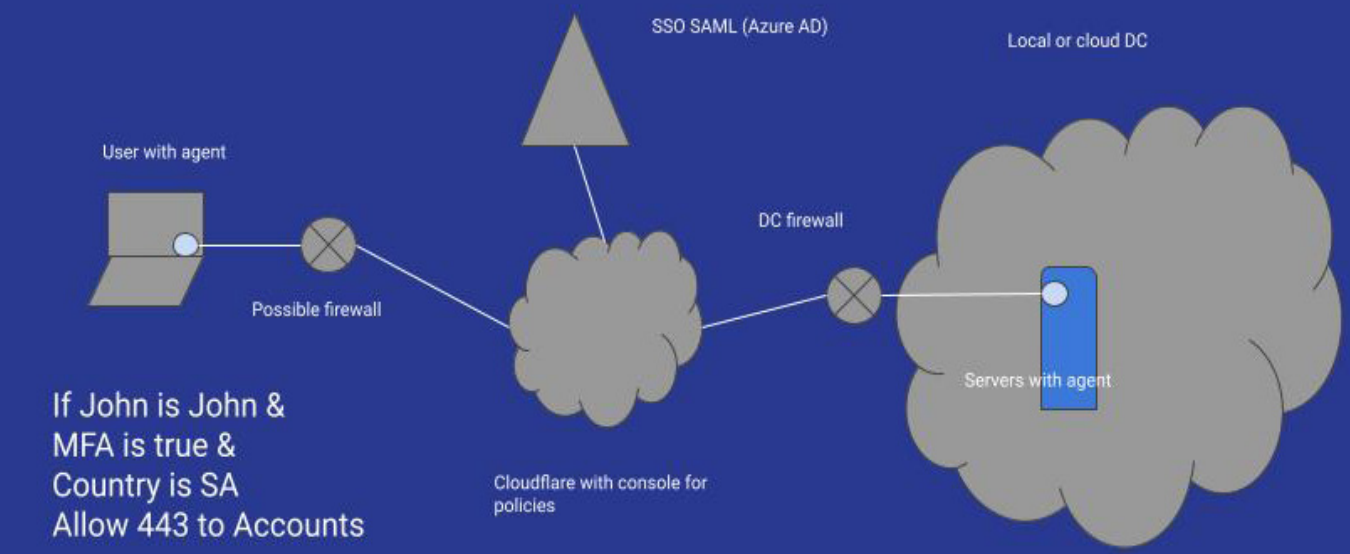
Zero trust architecture combines identity management, SASE and ZeroTier overlay networking

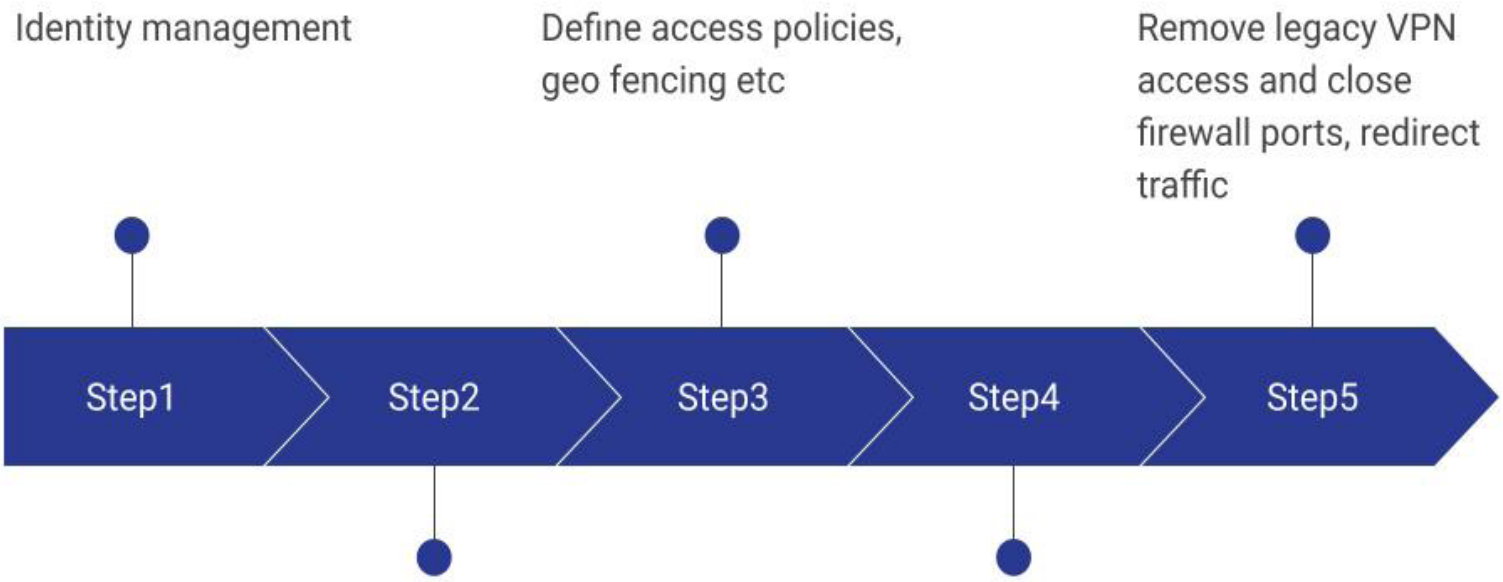
Our specific solution leveraged Cloudflare, a cloud based solution to wrap and deploy ZTA to legacy applications.

ZTA can also be deployed in house or by integrating separate products to achieve the same result.

Implementation

Deployment diagram





Impact

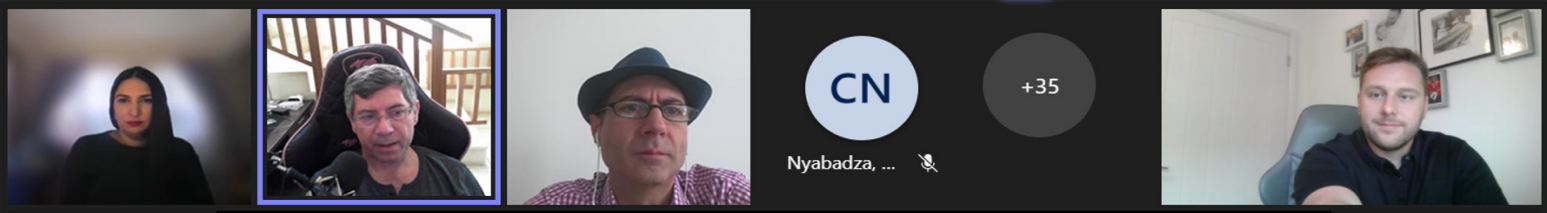
Firewall policy
Access audit
Insight reports

The firewall policy is now deny all inbound
There is one central place where all user access is logged
There is a single consolidated log of the access attempts

Access has to be explicitly allowed for it to happen, there is no assumed access to anything.

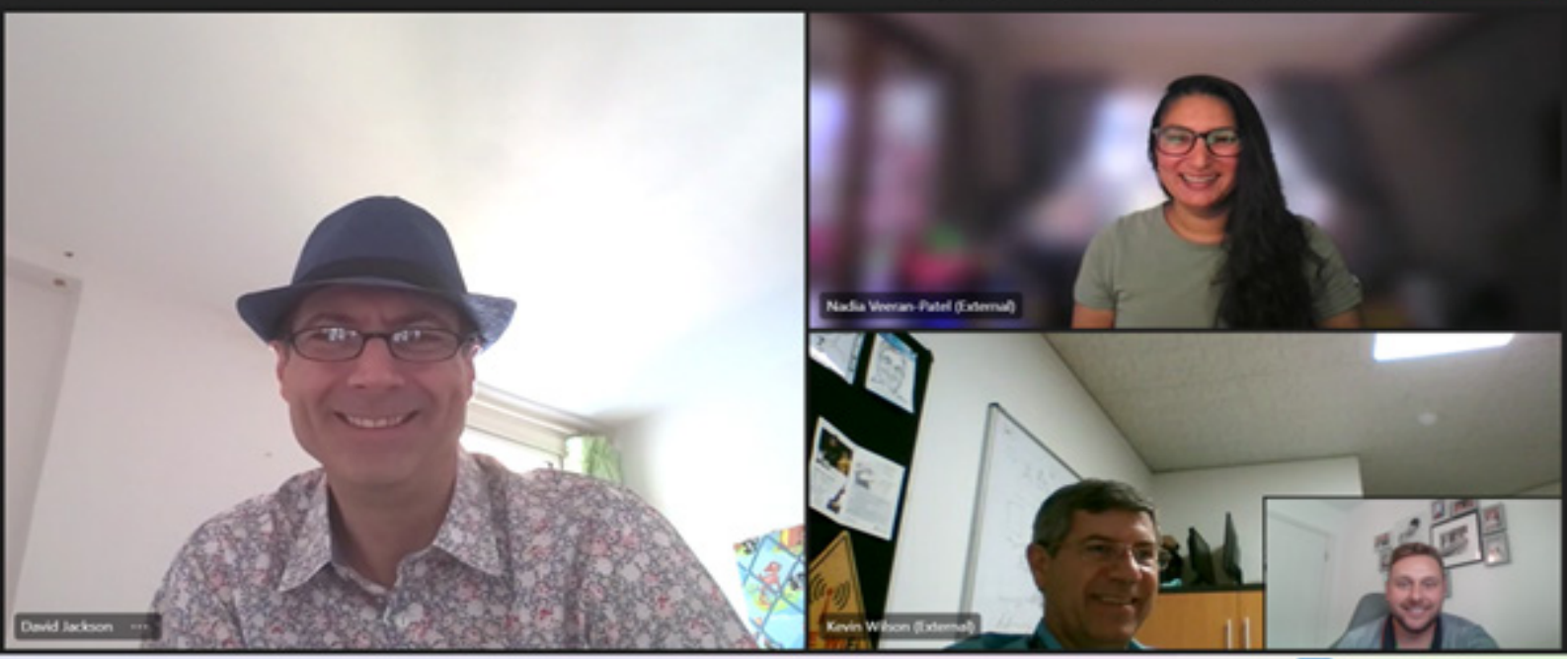
Users on the internal network cannot scan the network for exposed services

NAC (802.1) security for the physical layer stops rogue access to the network



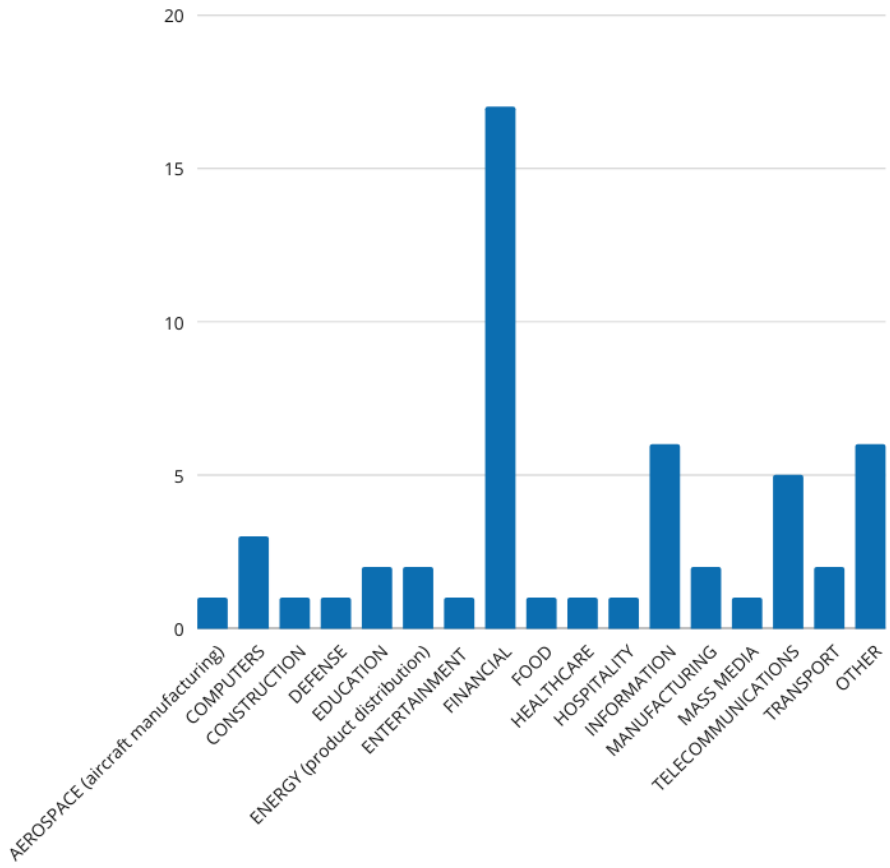
The problem

Future	Current	Problem statement
The ideal is to not trust anything or anyone by default. The focus is on users, assets and resources to determine trust, not static based parameters.	Most systems have defaults that assume a certain level of trust for locations or assets. Replacing those systems or standards with something that assumes no trust.	Putting Zero Trust into place needs to be carefully planned as the levels of assumed trust currently keep the business running.

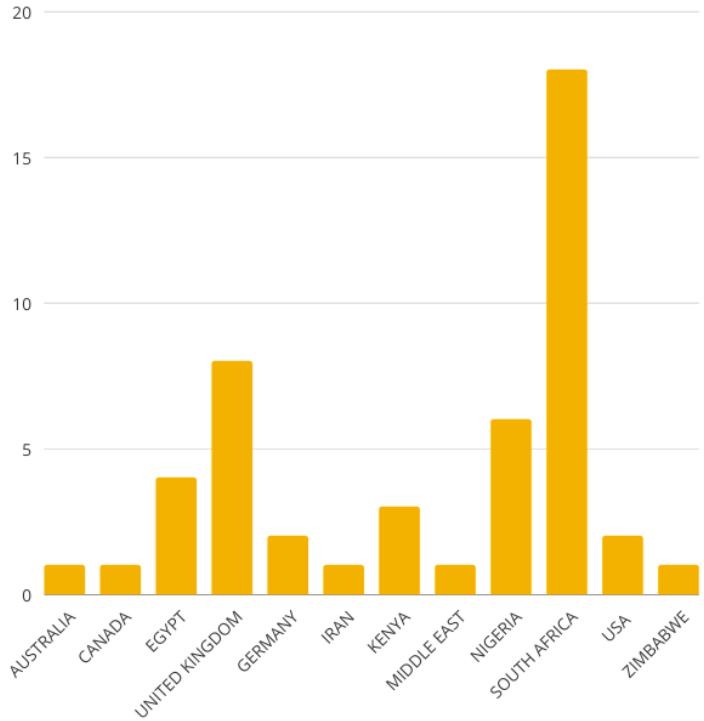


Who contributed to this intelligence?

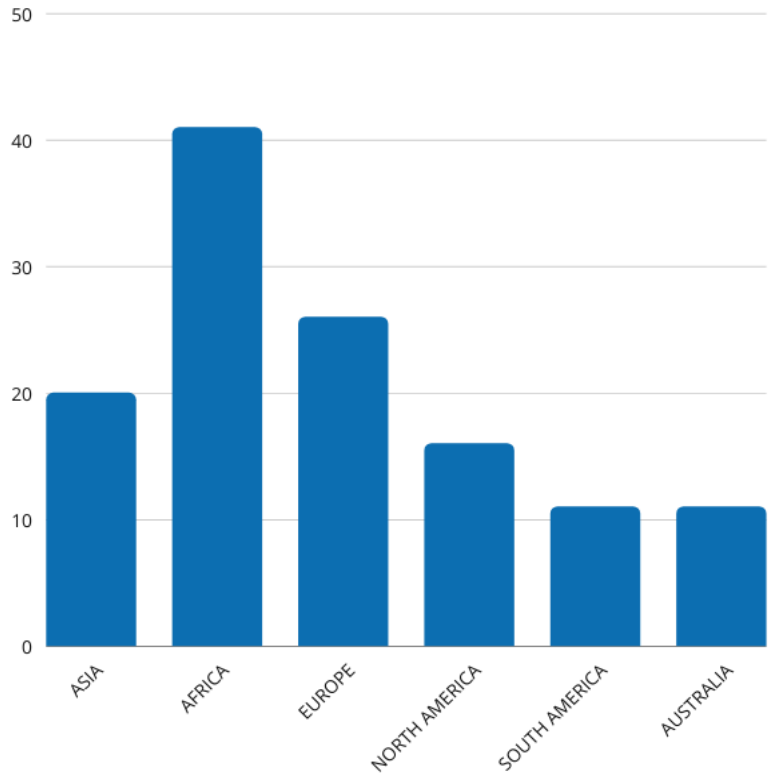
1. Defined Industry you work within



2. Country you are based



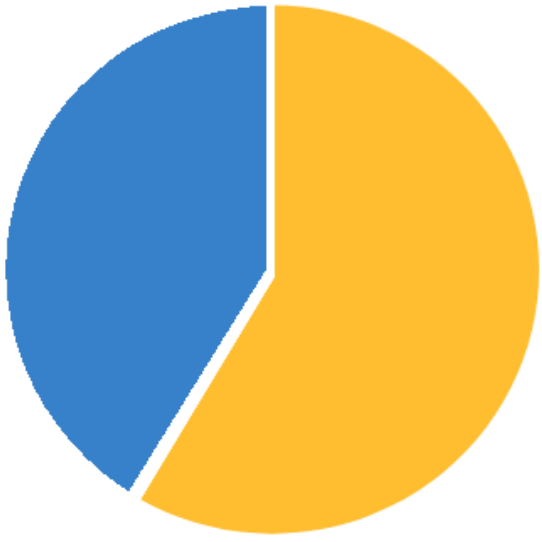
3. Active Operational Territories



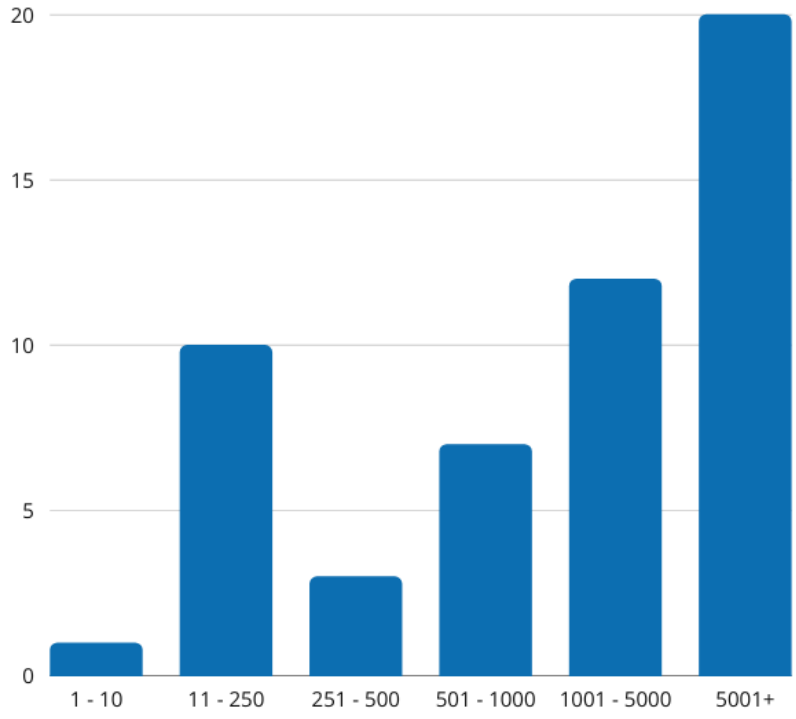
4. Are you Multi-National within these territories?

YES - 31

NO - 22

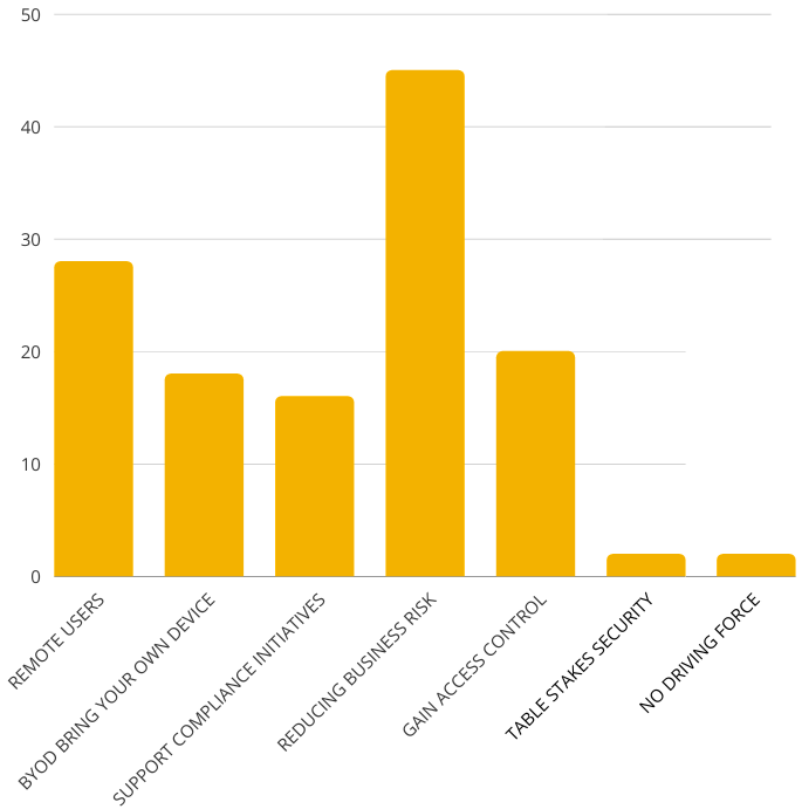


5. Size of Organisation by User Volume



Benchmarking materials

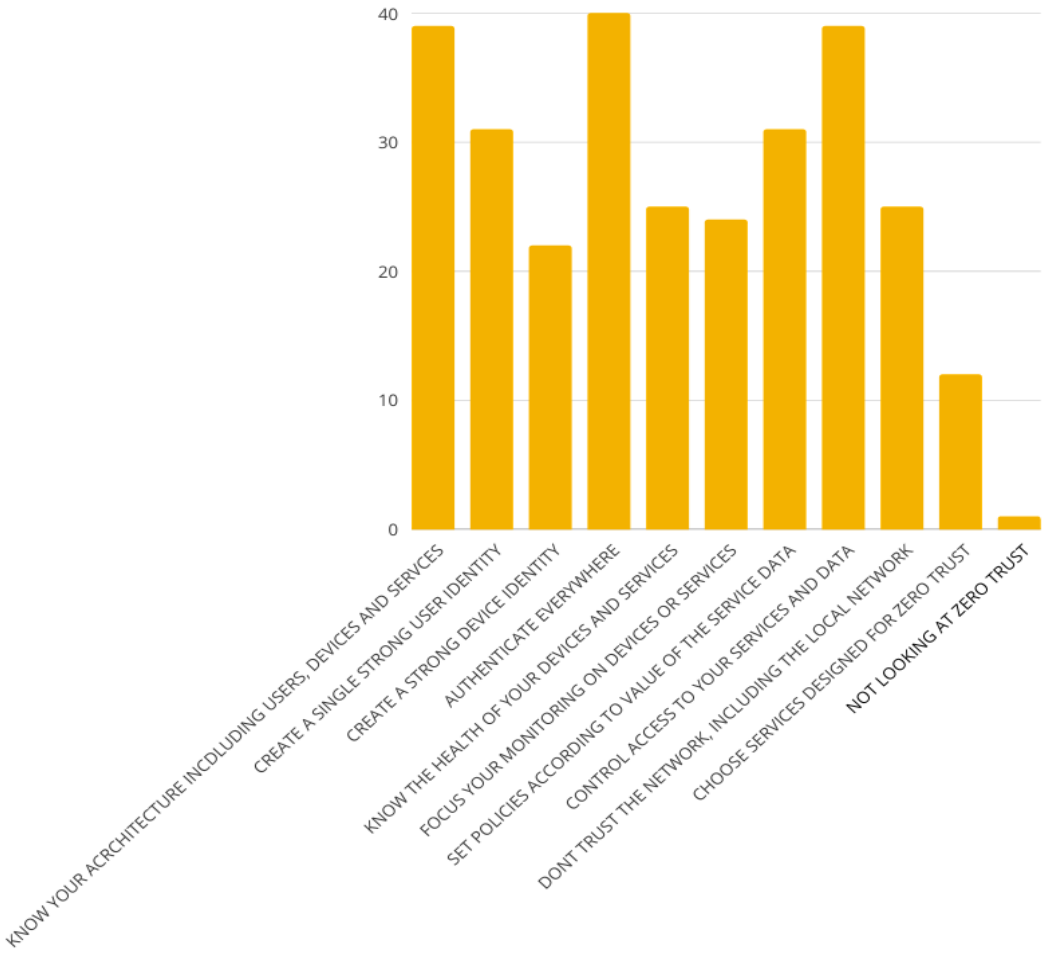
6. Driving force for implementing Zero-Trust



7. At what stage are you with the Zero Trust concept?

Investigating	-	41.5%
Implementing	-	43.5%
Undecided	-	15%

8. What principles have you considered along your journey?



Active Operational Territories - Africa, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Cisco
- M365
- Fortinet

Please elaborate on the pro's of your experience

- The zero trust approach and its principles
- What components comprise Zero Trust for the Workforce
- A practical approach in five phases for implementing Zero Trust for the Workforce

Please elaborate on the con's of your experience

- The challenges of each of the five phases
- How to measure success along your journey to Zero Trust for the Workforce

Active Operational Territories - Africa, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Zscaler
- Palo Alto

Please elaborate on the pro's of your experience

- Experienced implementation partners make a world of difference.

Please elaborate on the con's of your experience

- It's a programme not a project. Incremental security.

Active Operational Territories - Africa, Europe, North America.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Mostly, we make use of native cloud services. Much can be implemented with these when cloud native/based

Please elaborate on the pro's of your experience

- A lot is a matter of point and click. It's amazing to us that many (most) do not avail themselves of what's right there from each of the big 3 cloud providers

Please elaborate on the con's of your experience

- Proper, appropriate Monitoring gets expensive due to storage costs and premium IDS/XDR. Automating change control typically requires at least open source or commercial tool

Active Operational Territories - Africa, Europe, North America, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft - Azure AD, Azure AD Conditional Access, Azure AD MFA, MS App Proxy, Intune, Autopilot
- Privileged Access Management solutions
- Identity Management and Governance Solutions
- Host based AV, EDR, FW solutions
- SASE Remote Access solutions
- Micro-segmentation Solutions

Please elaborate on the pro's of your experience

- Access is centrally managed with a single identity using SSO
- MS conditional access policies allow who... where and when and with MFA if risk step-up is required
- Enforce posture assessment on corporate owned devices, all non-compliant devices are denied access to our network.
- Centralised policies that allow access to Intranet and Internet services including SAAS
- Identity based access to critical infrastructure and applications

Please elaborate on the con's of your experience

- Requires lots of solutions working seamlessly together.
- Often see config changes in one area affecting or defeating security controls
- Not so much tech related, lots of people change management issues.

Active Operational Territories - Africa, Asia, Europe.

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365

Please elaborate on the pro's of your experience

- Familiar products

Please elaborate on the con's of your experience

- None

Active Operational Territories - Africa, Australia

Please list the companies and products you have researched and the maturity of adoption from your research?

- Fortinet
- Netskope

Please elaborate on the pro's of your experience

- Seeing that the approach is similar but different at the same time

Please elaborate on the con's of your experience

- Not having extensive enough knowledge on implementation

Active Operational Territories - Africa, Europe.

Please list the companies and products you have researched and the maturity of adoption from your research?	Please elaborate on the pro's of your experience	Please elaborate on the con's of your experience
• Using existing native capabilities e.g. host-based firewalls and network firewalls etc. • RFI in progress for other tools	• Using existing native capabilities is: • Pros: relatively cheaper cost-wise than other tools on the market • Cons: Way too cumbersome and too complex to successfully rollout to the entire estate.	• Native capabilities are poor in terms of visibility and mapping application traffic flows, among other things

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?	Please elaborate on the pro's of your experience	Please elaborate on the con's of your experience
• Sophos, Fortinet, Trend Micro XDR	• Visibility of each user and data objects	• Heavy opex or capex investment and HR skills resources

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?	Please elaborate on the pro's of your experience	Please elaborate on the con's of your experience
• Implemented Microsoft O365 licenses.	• Reduced risks of Outlook phishing and password comprise.	• Resistance from users to comply with passwords requirements and expiry time from 180 days to 60 days and non reuse of passwords.

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?	Please elaborate on the pro's of your experience	Please elaborate on the con's of your experience
• Microsoft	• Still in the initial stages of research.	• Still in the initial stages of research.

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Fortinet
- ZTNA
- Undecided - Investigating

Please elaborate on the pro's of your experience

- They seem to have a good foundation for their technology

Please elaborate on the con's of your experience

- Well my concern with them is they seem to do everything

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft business premium, implemented
- Sophos, implemented

Please elaborate on the pro's of your experience

- Develop policy for identifying user access
- Enhances Data Protection compliance

Please elaborate on the con's of your experience

- Complicated
- Requires a change of ideology
- Not cost effective

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Cisco

Please elaborate on the pro's of your experience

- Smooth.

Please elaborate on the con's of your experience

- Resistance within the organisation.

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Fortinet
- Beyond Trust
- Palo Alto
- Cisco

Please elaborate on the pro's of your experience

- Review is ongoing

Please elaborate on the con's of your experience

- Review is ongoing

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365 - implemented
- Cisco - partial

Please elaborate on the pro's of your experience

- Microsoft carries a lot already in the box if you used M365 for office productivity

Please elaborate on the con's of your experience

- Cisco is between serving the old and the new. So the solution set not so clear cut if you already a Cisco shop

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Cisco
- Microsoft

Please elaborate on the pro's of your experience

- I briefly read about Zero Trust.

Please elaborate on the con's of your experience

- Not enough knowledge in the public domain.

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- E5 Security suite
- Cyberark
- Windows 365
- Azure PIM

Please elaborate on the pro's of your experience

- Much better, more granular access control and conditional access. Blast radius reduction etc

Please elaborate on the con's of your experience

- Admin-heavy and requires staff to operate, monitor and administer

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- MSFT

Please elaborate on the pro's of your experience

- Use of dynamic policies is not sufficient

Please elaborate on the con's of your experience

- Static

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Embed AI preventative capabilities, focusing on behaviour, access and identity regardless of where user based

Please elaborate on the pro's of your experience

- Pros - moved to proactive defence capabilities and data usage... cons initial time to ensure budgets could be secured

Please elaborate on the con's of your experience

- Getting the business to understand proactive capabilities requires a different budget strategy was tough
- Ensuring brining the business units heads along. 6mnths later and we couldn't do without it.. Value proposition has been out of this world

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365
- Cybereason
- Paloatlo
- Forcepoint

Please elaborate on the pro's of your experience

- M365 - single pane on Endpoint and Service Management.

Please elaborate on the con's of your experience

- Product Commercials are based on risk appetite

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365 E5
- CISCO
- CLOUDFLARE

Please elaborate on the pro's of your experience

- Still investigating

Please elaborate on the con's of your experience

- Still investigating

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Palo Alto
- M365
- Yubikey

Please elaborate on the pro's of your experience

- Still investigating

Please elaborate on the con's of your experience

- Still investigating

Active Operational Territories - Africa

Please list the companies and products you have researched and the maturity of adoption from your research?

- Dark Trace for End users - implemented
- Moving to E5 microsoft licence

Please elaborate on the pro's of your experience

- Flagging things we didn't know about

Please elaborate on the con's of your experience

- Expensive

Active Operational Territories - Australia, South America, North America, Europe, Africa, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft, Part of license, implemented
- Cycognito Attack Surface Management Platform, implemented

Please elaborate on the pro's of your experience

- MS is delivered, so why not use it?
- Cycognito has a 360 degree approach that fits for us.

Please elaborate on the con's of your experience

- none

Active Operational Territories - Australia, Europe, Africa.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Part of E licence for M365
- CyberArk
- Cisco ISE

Please elaborate on the pro's of your experience

- Hybrid approach, depending on the privilege of the identity

Please elaborate on the con's of your experience

- Especially in the SA the pricing and budgets are restrictive. as well as local skill to support. investigating XaaS as an option

Active Operational Territories - Australia

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365 e license

Please elaborate on the pro's of your experience

- Less risk

Please elaborate on the con's of your experience

- Annoys users can impact remote access especially development of new code

Active Operational Territories - North America, South America, Europe.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Secure Remote Access
- Cisco

Please elaborate on the pro's of your experience

- PROs: security
- CONS: extra cost (which should be compared with the cost of a

Please elaborate on the con's of your experience

- No experience so far

Active Operational Territories - North America, Europe, Asia, Australia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- VMWare
- Cisco

Please elaborate on the pro's of your experience

- N/A

Please elaborate on the con's of your experience

- N/A

Active Operational Territories - Europe, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Still investigating

Please elaborate on the pro's of your experience

- Still investigating

Please elaborate on the con's of your experience

- Usual vendor overload. Poor clarity on offerings

Active Operational Territories - Europe, South America, North America, Asia, Africa.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Guardicore
- Istio mesh
- Kong gateway for APIs

Please elaborate on the pro's of your experience

- A few solutions can be used to help with service mapping. Implementing zero trust in some pilot scenarios allowed for more flexibility in having a less complex network architecture and account management in cloud

Please elaborate on the con's of your experience

- Early days in investigation but common theme is that you need to have a detailed understanding of all services / components you own and the relationship between them before even attempting zero trust

Active Operational Territories - Europe, Asia, South America.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Okta
- identity
- Still researching

Please elaborate on the pro's of your experience

- Limited experience, just starting

Please elaborate on the con's of your experience

- As above

Active Operational Territories - Europe.

Please list the companies and products you have researched and the maturity of adoption from your research?

- M365
- Cisco

Please elaborate on the pro's of your experience

- None

Please elaborate on the con's of your experience

- None

Active Operational Territories - Europe

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft stack (E5 licensing) inc Defender/ InTune - mid-deployment
- Akami EEA - mid-deployment
- Thycotic - selective deployment

Please elaborate on the pro's of your experience

- Microsoft tech stack - well integrated providing good coverage from multiple angles and layers.
- Akami EEA - Easy for staff to use, provides a simple way of protecting remote access

Please elaborate on the con's of your experience

- Microsoft tech stack - can be complicated to implement, licensing requirements for 'the good stuff'
- Akami EEA - local jump hosting can be tricky
- Thycotic - requires knowledge and admin overhead to use effectively

Active Operational Territories - Europe

Please list the companies and products you have researched and the maturity of adoption from your research?

- Consider using a robust framework and tried concepts over zero trust.

Please elaborate on the pro's of your experience

- Tried and tested approach is well understood and resonates with Board. No one of any senior significance subscribes to or understands zero trust. Take a different approach.

Please elaborate on the con's of your experience

- As above.

Active Operational Territories - Europe

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft E5 plus security

Please elaborate on the pro's of your experience

- Single pane of glass
- Good integration between products
- Good reporting breach, but is money anyway)

Please elaborate on the con's of your experience

- Cost

Active Operational Territories - Europe, Asia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- ZScaler
- Forescout.
- M365

Please elaborate on the pro's of your experience

- Too many to list.

Please elaborate on the con's of your experience

- Expense. Getting NAC implemented for post connect to pre connect.

Active Operational Territories - Asia, Europe, North America.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Microsoft Azure

Please elaborate on the pro's of your experience

- Use Microsoft Authenticator for MFA
- integrate with B2B partners seemlessly
- Use Microsoft Sentinel and Defender
- Enable securtiy policies

Please elaborate on the con's of your experience

- Very limited way to customize the login experience and profile setup

Active Operational Territories - Asia, Africa, Europe, North America, South America, Australia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Netskope
- Tessian
- Beyondtrust

Please elaborate on the pro's of your experience

- Clarification regarding complexity and pitfalls/constraints

Please elaborate on the con's of your experience

- Underestimating the complexity of systems environments and inability to pivot and meet specific challenges.

Active Operational Territories - Asia, Africa, Europe, North America, South America, Australia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Beyond trust
- E5

Please elaborate on the pro's of your experience

- None too premature

Please elaborate on the con's of your experience

- None too premature

Active Operational Territories - Asia, Africa, Europe, North America, South America, Australia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- MS
- AWS
- IAM provider (withheld)

Please elaborate on the pro's of your experience

- Resilience risk reduction
- Improved IAM lifecycle management
- Enable BYOD

Please elaborate on the con's of your experience

- Obsolescence application management
- Network reorientation and micro segmentation changes

Active Operational Territories - Asia, Europe, North America, South America, Australia.

Please list the companies and products you have researched and the maturity of adoption from your research?

- Part of E license

Please elaborate on the pro's of your experience

- N/A

Please elaborate on the con's of your experience

- N/A

Active Operational Territories - Asia

Please list the companies and products you have researched and the maturity of adoption from your research?

- Assessment of posing risk due to network connections can reveal the high risk areas; thereafter, zero trust -which is among risk mitigation controls in such case- can be planned.

Please elaborate on the pro's of your experience

- Zero trust dramatically reduces applicability of network breach.

Please elaborate on the con's of your experience

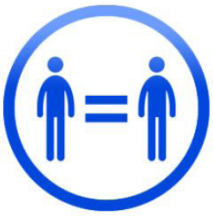
- As far as coms to mind, controls placement and practice requires time, money, energy.

WHAT TO EXPECT

CISO Alliances

Alliances - A union formed for mutual benefit
Everyone is expected to contribute

Access to a community of peers to benchmark, support and debate



Non-discriminatory community on race, gender, age, vertical experience

Community First, Commercials Last

An opportunity to engage on the Chat forum, Digital Alliances Chapter and Physical Chapters

WHAT WE EXPECT

This is a supportive environment for progression and growth

You do not directly benefit from topics being raised but, have experience within the topic:
1 - Share your knowledge
2 - Bring forward themes / topics that matter to you and your business objectives

Suggest and recommend peers to broaden the perspectives within the group

Constructive comments rather than opinionated are provided. Back up your opinion

If there is a potential eventuality of commercial gain for the organisation you work for, you will be expected to pay to play to help sustain the Alliances and their activities.

THANK YOU
WE HOPE YOU ARE ENJOYING THE JOURNEY