CISO Alliances

Nairobi Chapter

30th June 2023

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

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’

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Executive Business Exchange

DPO Alliances

CIO Alliances

CISO Alliances

CXO Alliances

CMO Alliances

CDO Alliances

CISO Alliances

Foreword

Karibu Team,

It is great to once again be back in NBO for todays in person CISO Alliances Nairobi.

The pandemic has naturally shifted the way of thinking, BCP and the adoption of the 'virtual' world, so I would like to firstly thank you for your continuous involvement as community members and your time investment into attending today's chapter.

As we all know the threat landscape is an ever-evolving space where we as a group of IT and Infosec leaders are either one step ahead or one step behind the threat actors.

Today's agenda has been formulated around the issues highlighted by you as a group, so please do continue to influence and advise.

The CISO Alliances mantra is to ensure that these end user driven meets, are purely focused around the educational and requirement needs of everyone involved.

With you all having security and operational responsibility 'Protecting the 'Crown' Jewels', the aim of today and future programmes is to share best practice, benchmark strategies and more importantly have very open and candid debate around issues and being faced.

All CISO Alliances activities operate under strict Chatham House Rule to ensure we have a trusted and confidential environment.

Without sounding like a Roman Emperor this a 'for the people, by the people' initiative so I actively encourage open debate and opinion throughout the day.

I look forward to a very insightful afternoon.

Asante,

Phil Manny

Regional Director – CISO Alliances Egypt | Ghana | Kenya | Nigeria

12:00

Registration and Networking

12:45

Group Networking Lunch

14:00

Welcome Remarks and Housekeeping

Phil Manny, Director – CISO Alliances

14:05

Session 1 - Group Workshop

"ZT or Not ZT.... That is the question...."

15:05

Networking Break

15:20

Session 2 - Open Forum

Are your offices becoming Internet cafes?

Edwin Sutherland, Principal Architect – Cloudflare

16:00

Debate and Q&A

16:10

Session 3 - End User Perspective

"The Journey to Zero Trust"

Session Moderator: Cephas Okal, Head of ICT – Sumac Microfinance Bank Ltd

Panellists:

- Eric Ngei, Senior Manager, Cybersecurity – KCB Bank Group
- Edwin Sutherland, Principal Architect – Cloudflare
- Joan Mburu, CISO – Airtel Kenya
- Ferdinand Ragot, IT Manager – Inchcape Kenya

17:15

Post Alliances Networking

CISO Alliances

Chapter Agenda

CISO Alliances

Nairobi Chapter

June 2023

Chapter Partner

CLOUDFLARE

Use Case Partner

CLOUDFLARE

Edwin Sutherland
Principal Architect
Cloudflare

Ayode Akinfemiwa
Account Executive SSA
Cloudflare

Graham Turnbull
Account Executive SSA
Cloudflare

Cem Lacin
Business Development
Representative SSA
Cloudflare

Chad Toerien
Account Executive SSA
Cloudflare

CLOUDFLARE

Protection in every direction

One global platform secures employees, applications and networks. Everywhere Security.

275+
Cities in 100+ countries, including mainland China

22
African PoPs

126B
Daily threats blocked

95%
of world's Internet users within **50ms** of our network

cloudflare.com

Community Attendees

Alfred Maina
Head of IT
Tsavo Real Estate Investment Company

Allan Rono
Senior Manager,
Information Security Risk - Africa
Standard Chartered

Anthony Nthiwa
IT Infrastructure Manager
CMC MOTORS

Beatrice Wagate
ISSM
Sarova Group

Bernard Omware
CIO
Kenya Wildlife Service

Cephas Okal
Head of ICT
Sumac Microfinance Bank Ltd

Chumari Wachaga
Group Head of IT /CIO
AutoXpress Group

David Kitonga
Global IS Manager
Oxfam

Dennis Rono
Manager - IT Operations
AutoXpress Limited

Community Attendees

Emily Muragari
Consultant, Information Security
Transunion Bank

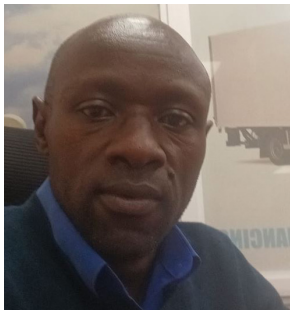
Emmanuel Mose
ICT Lead
African Economic Research Consortium

Eric Ngei
Senior Manager, Cybersecurity
KCB Bank Group

Ferdinand Ragot
IT Manager
Inchcape Kenya

Fredericks Yambo
Head of ICT - East Africa
Gatsby Africa

Godfrey Machio
Data Protection Officer
Family Bank



James Tindi
ICT Infrastructure and Security Lead
Sumac Microfinance Bank

Joan Mburu
CISO
Airtel Kenya

Joel Nderitu
Head of IT
Goodlife Pharmacy

Community Attendees

Kevin Kanyi
Global Head of Threat Intelligence & Threat Hunting
M-KOPA

Paul Karimi
Head IT Risk, Security and Governance
Old Mutual East Africa

Rittah Okal
Frequency Spectrum Data Management Officer
Communications Authority of Kenya

Tom Mboya
Technology Lead, East Africa
Unilever

Stanley Githae
Head IT
Chai Sacco Society Ltd

Workshop

Session 1

“ZT or Not ZT…. That is the question”

Session Overview and Synopsis:

- We will kick start the day with a group workshop where we divide into sub-groups. The objective of this workshop is to provide participants with a comprehensive understanding of the Zero Trust security model and its implementation in an organization. Through interactive discussions and exercises, participants will learn about the principles, benefits, and key components of Zero Trust, as well as how best to develop a Zero Trust strategy for their organization.

Takeaways

ZT or Not ZT... That is the question....

During the group workshop we split the participants into teams and conducted a gamification exercise to unpack different vantage views.

Question 1 - What is the main problem with the traditional perimeter-based security model?

Outcomes and debated areas

- We are now encountering situations where the modern way has changed. i.e The analogy of the comparison between a traditional and modern car
- The traditional perimeter-based security is static in nature
- The traditional perimeter does not consider new threats, stakeholders nor WFH
- Insider threats — how do you defend against what's already inside?
- Security is no based on ability to change – Previously based on Previously based on ACL (Access Controlled List)
- We need to now focus on as little access as possible
- Inability to define new threats
- In a traditional model you create a safe area - All 3rd party externally posing a threat, where every access needs verification
- Tunnelling past your own defenses

Question 2 - How does the Zero Trust model address the limitations of the traditional model?

Outcomes and debated areas

- ZT looks at situations where you are trying to prevent and polices so that a user needs to go through the necessary criteria e.g the analogy of hotel door access
- "Trust NO one – Verify everything"
- ZT enables SOD (Segregation/Separation of Duties)
- Continuous authentication and verification of user
- Reduces risk of lateral movement through the continuous asking of "who are you?"

Question 3 - How would you approach developing a Zero Trust strategy for your organization?

Outcomes and debated areas

Firstly understand who is in charge of cyber security?

- Is it the CEO in charge, responsible and accountable?
- Factor in who defines budget, policy and procedures around cyber?
- Once buy in from management is achieved you can then choose solution relevant to your entity
  - ➢ i.e 50 vs 1000 staff, Govt. or Private, Cloud vs. on prem infrastructure

- Classify and identify risk appetite – Look at the severity as a matter of priority
- Define what are your assets and understand what needs continuous monitoring and protection
- Understand existing technology infrastructure and define architecture with least privilege access using different techniques e.g. RBAC – Role Based Access Control

Takeaways

Question 4 - What are some of the key considerations when selecting technologies and solutions for implementing Zero Trust?

Outcomes and debated areas

- There are many solution are available so it is hard to decipher
- This needs to be linked in to the type of organization as it is dependent on the specific part of the infrastructure that is being worked on
- ZT is not here to replace but to complement and enhance what you have
- The solutions need to be open and readily integratable with existing security infrastructure
- ➢ Consider threat intelligence capabilities – Not all have CAPEX for in-house SOC, Managed Cybersec or multiple security solutions
- ➢ Ability to support IDP solutions for SSO capabilities
- ➢ Scalability?
- ➢ Ability to support remote working?
- ➢ Ease of use – Functionality vs. Simplicity (Too much control reduced usability)

- Visibility of solutions, how automated and how current needs to be considered

Define technological requirements:

- ➢ Dependent on hybrid, cloud or on prem
- ➢ Every vendor has key strengths – We need to combine the best stack, as too much control reduces usability

Question 5 - How do you think implementing Zero Trust can improve overall security posture and protect against emerging threats?

Outcomes and debated areas

- Reduction in threat surface
- It provides identification and access needs for all who need PAM
- At every point there is an element of resilience through the segregation that ZT encompasses
- Operationally it improves experiences as there is 1 single pane (Orchestration Dashboard) for ease of use and management – This enables full visibility of solutions, flexibility and increased productivity
- Threat Intelligence feeds helps gather information about threats more quickly and efficiently, filtering out false alerts, and speed up triage.
- The element of continuous verification reduces exposure risk

Takeaways

Open Forum

Session 2

Are your offices becoming Internet cafes?

Session Leader

Edwin Sutherland, Principal Architect – Cloudflare

Session Overview and Synopsis:

In the wake of Covid-19, many businesses shifted their operations from having employees in offices to working from home. Remote Access VPNs proved cumbersome for users and, on the contrary, a threat vector to businesses. The emergence of Zero Trust Access quickly caught CISO's attention, and many are now in the adoption phase of SASE and Zero Trust solutions. This session explores the transformation of corporate networks from location-based access to a borderless Zero Trust Access model.

Session Outcomes and Takeaways:

The following core themes will be covered:

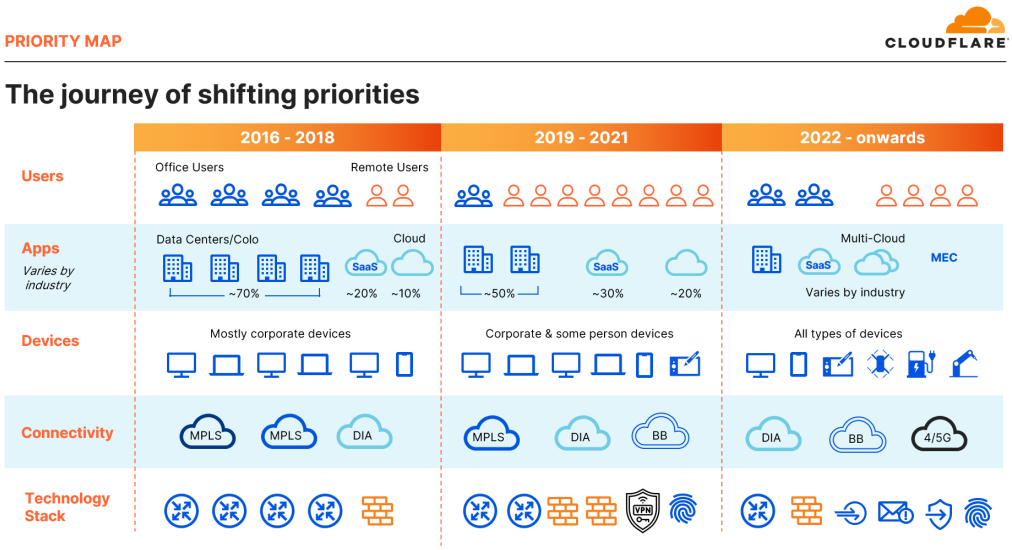
- Always on Security
- Location awareness but not location dependent
- Device-agnostic access
- Least privilege access
- Performance optimized access

Takeaways

Edwin led a quirky and relevant discussion around “Are your offices becoming Internet cafes?”

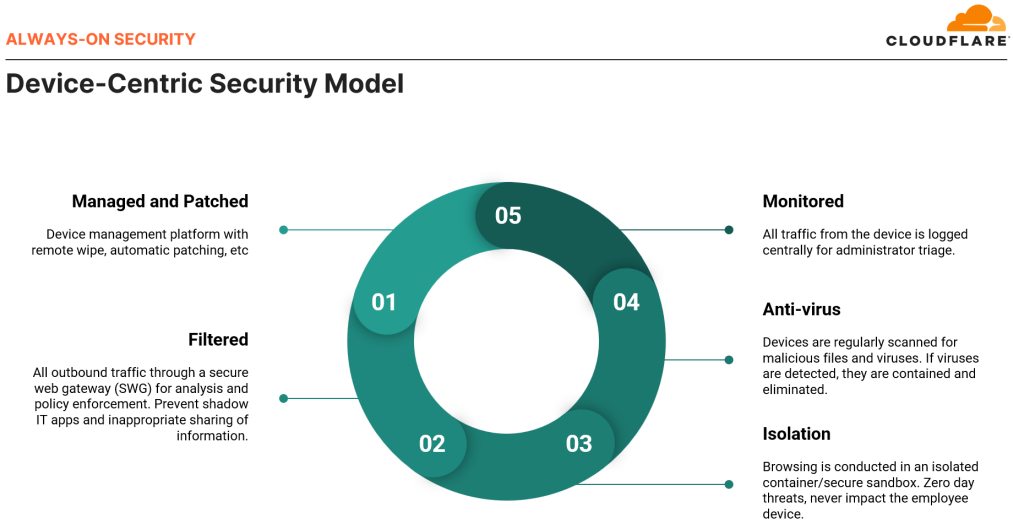
Agenda:

1. The journey of shifting priorities
2. Always-on Security
3. Embrace Zero Trust
4. Secure Internet Traffic
5. Enhance User Experience



Priority Map - Let’s evaluate security implications

- How will we continue to protect remote workers’ access to internal resources without slowing them down?
- What security controls do we still need at our branch offices, and which investments no longer make sense?
- How can we retain visibility of employee activity with so many modes of connection?
- How can we achieve consistency in our security model, and route traffic without unnecessary hops?

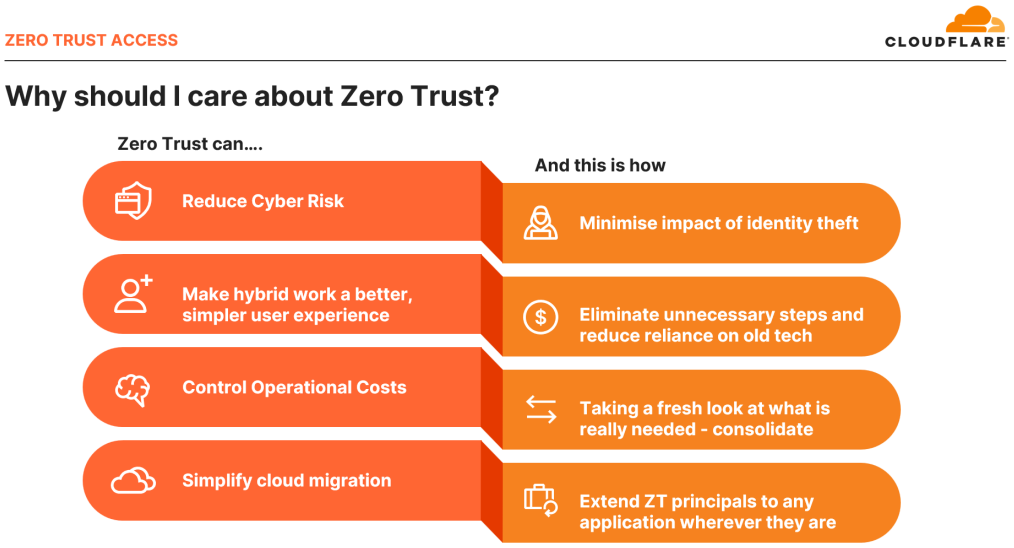


Tip: Focus your security strategy on **employee devices**, not office locations.

Takeaways

ZT Access

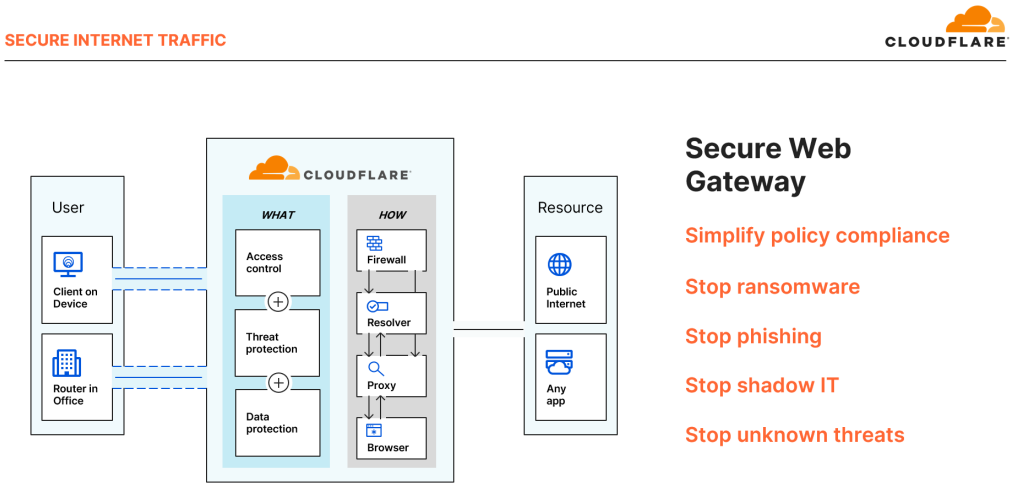
- Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating digital trust from an organization.
- Rooted in the principle of “never trust, always verify, least privilege”
- Zero Trust strategy is decoupled from technology, so while technologies will improve and change over time, the strategy remains the same.



Tip: With contextual access controls, you can ensure that only managed devices can access specific apps and data.

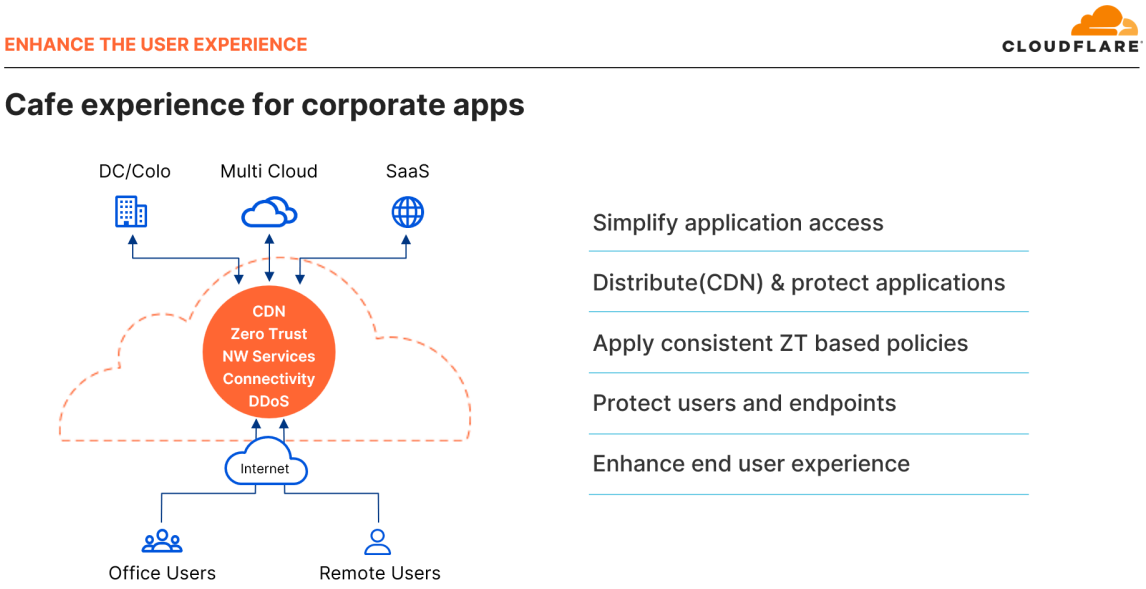
Secure internet traffic

- Historically, branch offices sent Internet bound traffic to primary DC for hardware based security inspection and enforcement
- With applications shifting to the cloud and users no longer at branches this model is not efficient
- Legacy hardware firewall appliances were not built for the constantly- evolving threat landscape of the modern Internet



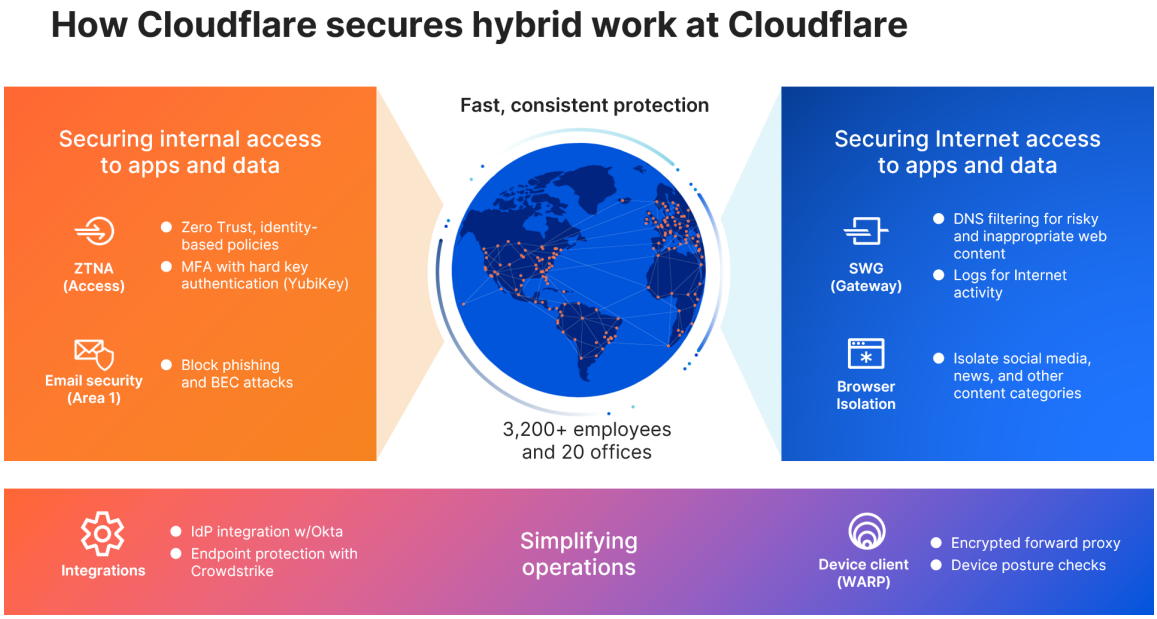
Tip: Set corporate policies for Internet use and **filter out malicious or inappropriate sites** in a consistent manner.

Takeaways



Tip: With **contextual access controls,** you can ensure that only managed devices can access specific apps and data.

How does Cloudflare Secure Cloudflare?



Useful Links

Download the complete Roadmap to Zero Trust Architecture - cfl.re/architecture-roadmap

DDoS threat report for 2023 Q1 - https://blog.cloudflare.com/ddos-threat-report-2023-q1/

Takeaways

Questions posed:

Q. How does Cloudflare give help with DDos attacks?
ES: Provides DDos protection specifically to application as Cloudflare do this naturally to protect our own business. We can also sit in front of public applications. DDos attacks are distributed due to the variety of Cloudflare location, therefore only clean traffic come into the network even with layer 3, 4 or 7 attacks.

With our 192 TB per second capacity inherent results are achieved as each of our 300 locations act as a scrubbing centre

Q. Do you need a device in the network and how easy it it to get solution on a device?
ES: You can get started initially with deploying zero trust agent and other foundational endpoint security solutions on corporate laptops, and mobile devices, securing access to SaaS applications and Internet usage. You can then expand this to cover access to self-hosted applications as a next step.

Q. Can you paint a picture of how locations with look as we expand with new offices/location?
ES: In this near architecture of treating offices as a glorified Internet cafe, the focus shifts from building security boundaries in office locations to user endpoint devices. Thus all users' devices should be managed and monitored as the source of entry to corporate resources access regardless of user location. The office network loses its importance and you gain consistency in your security policy enforcement independent of location. Effectively wherever users go the security policy follows them. As a side effect you'll find that the need for a corporate WAN also becomes less as your application landscape shifts away from the Data Center to the Cloud.

End User Perspective

Session 3

“The Journey to Zero Trust”

Session Overview and Synopsis:

In this session, we will embark on a journey to Zero Trust, a paradigm shift in cybersecurity that challenges traditional perimeter-based security models. Our panellists will discuss through the key stages of this transformative journey, highlighting and debating the necessary steps, considerations, and best practices for successfully implementing Zero Trust within an organisation.

Moderator: Cephas Okal
Head of ICT
Sumac Microfinance Bank Ltd

Eric Ngei
Senior Manager Cybersecurity
KCB Bank Group

Joan Mburu
CISO
Airtel Kenya

Edwin Sutherland
Principal Architect
Cloudflare

Ferdinand Ragot
IT Manager
Inchcape Kenya

Takeaways

During the panel discussion our esteemed panel led by Cephas Okal conducted an interactive impromptu conversation around the journey to zero trust. This included the integration of audience participation resulting in a room wide exchange of thoughts.

Discussed areas

Question: What runs through an IT leader mind from a ZT perspective?

- We must understand our crown jewels and know what we are protecting
- Ensure our users and assets are secure through micro segmentation and privileged access
- It is not so much a distraction but creates an understanding of our environment and the ability to lock down as much as possible.
- If you have international geolocation its important to have partnerships in order to extend reach

Question: How do you shift With the mindset of ZT, and sell the board for buy in?

- How is best to 'sell' the concept to the board in order create 'buy in'?
- If you don't position yourself early enough this will cause a pain

i.e. Due diligence isn't done when assessing what type of critical/sensitive application it is and whether it should be internet facing

- There is a need for acrobatics (WAF etc) as otherwise it can result in a serious and bitter discussion with a vendor to get extra things done
- The agility of of ZT is a benefit as this enables faster movement to the cloud
- ZT is not as expensive as on-prem and dealing with end of life solutions.
- We need to sell the vision and future as if all, which can be challenging if all on-prem

Takeaways

How does ZT manage users but not disrupt quality?

- It is important to explain why ZT is essential and expose the experience user will receive
- Emulate the experience to show what is looking to be achieved with limitations – communication and awareness to users is key
- It is important to whitelist applications by identifying critical ones and double checking each platform a user needs and is trying to access.

AI and machine learning as an emerging trend in ZT

- There is space in ZT to develop more intelligent platforms to save on manual work i.e. Trawling the internet to blacklist malicious sites
- On the flip side tech is here to stay - so we must be aware of the information and data sharing with AI systems to prevent abuse/oversharing which can result in compromise.
- Are there encryption standards?
- Post quantum systems
- How to handle personable data and privacy – We need to adopt anonymising of data/ pseudonymisation
- DLP – restrict exposure by either blocking or reduct of data (not just text but imaging data

Advice to those starting the ZT journey

- ✓ ZT is a humungous new trend – ensure you don't bit too much to chew
- ✓ Even vendors need to catch up so don't rush if you need to replace on-prem
- ✓ Start small and create a vision
- ✓ Get someone to help build the road map (This can be a challenge if using a vendor as there is commercial element)
- ✓ Align roadmap to IT strategy
- ✓ Create your identity and slowly move away from legacy
- ✓ Select the right solution for integration
- ✓ Have your foundations in place - Create a framework to do an assessment, either by yourself or in collaboration with a consultant (This can help understand risk strategy)
- ✓ Use data as opposed to 'big words' to convey the benefits and engage with the business
- ✓ Remember ZT is a not a product but a mind shift and strategy – It is not just a 'shiny' tool to solve the problem as it is only as good as the person who uses it

Additional discussion areas:
What would you remove as you go to ZT?

ZT applies the security principle of IAAA (Identification, Authentication, Authorisation, Accountability) and is imperative that you understand your environment and architecture.

In a best practice ZT would complement any security solution that covers the same security principles but works in silos. Always map out your architecture from a SASE and ZT convergence point of view.

e.g. XDR will ZT capabilities

Takeaways

On the journey how are we able to achieve visibility and gain assets?

- Integration with SIEM
- Device management – To understand where they came from
- Profiles and components – ability to build profile or all infrastructure assets, monitor and then devise out a response

How can security, IT and management work together due to the view of cyber security being a cost centre?

- Create analogies, stories and speak language of non-technical i.e. A Ferrari can travel at 350km per hour but would this be done if it has rubber brakes
- Show compliance examples and the impact it has and could have on business through hard facts
- Simulate a crisis situation for visuals
- Understand financial literacy language, e.g. Full OPEX/CAPEX how it affects TCO (Total Cost of Ownership), Amortization, Depreciation when focused on hardware/license purchases, monthly costs, contracts & SLAs and how each will impact the business bottom line

Useful link: **https://www.linkedin.com/posts/bouchernicolas_capex-vs-opex-do-you-have-a-hard-time-defining-activity-7048916212633751553-QzXM/?utm_source=share&utm_medium=member_desktop**

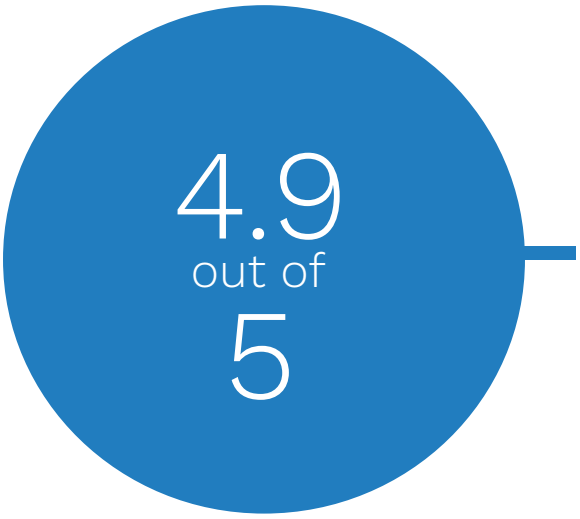
Takeaways


CISO Alliances
CLOUDFLARE
Everywhere Security
CISO Alliances
CLOUDFLARE


SO Alliances
Nairobi Chapter
30th June 2023
Chapter Partner
CLOUDFLARE
Everywhere Security

Chapter Scores

Chapter Overall Experience
Scored by the Community

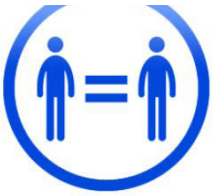


Chapter Format Scored
by the Community

WHAT TO EXPECT

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