



The unpalatable truth about Zero Trust

Chris Trynoga
Senior Solutions Engineer
ctrynoga@akamai.com



Don't Panic!

- The slides don't contain a lot of text
- I will show a summary after each topic
- For questions, please write them down and ask at the end

Thanks =)



The key Zero Trust principles

The key Zero Trust principles

- all entities are untrusted by default
- least privilege access is enforced
- comprehensive security monitoring is implemented





Lessons from the past

Lessons from the past

- Allow-listing is not a new concept...
 - ...but have you tried applying it?
 - For devices?
 - For applications?
 - For websites?
- How do you know where and how to apply the policies?
 - Need to know all your (critical) assets
 - Need to know the (security) state of them
 - And now just monitor all behavior and make sense of it!
 - Bonus Points: Be able to selectively block at any moment!





What has changed?

What has changed?

- Well, a lot more computing power, and faster internet!
 - (which we mostly use inefficiently, but that's not today's topic)
 - This enabled us new technical options
 - Think about stuff like SIEM, EDR/XDR available for everyone...
 - ...or any other fancy ML / AI / Big-Data technology
- So, everything is good now?
 - No
 - Nope...
 - The same struggles as before exist
 - AI doesn't help us to create an asset inventory
 - SIEM, EDR and XDR only cover monitoring as a ZT principle





What has changed? Part 2: Something positive!

What has changed? Part 2

- Example 1: ZTNA
 - Or: why should a remote device need full network access?
 - Or: why should any device need full network access?
 - Works well because our daily business tools are web-apps now
 - Session-based, strong authentication, cloud-ready
 - Requires good network speed, and has CPU overhead
- Example 2: Segmentation
 - Or: why should any device need full network access?
 - “Classic” centralized approach not working anymore
 - Good network connectivity allows for a decentralized approach
 - Each device has enough compute to enforce on its own
 - Each device is assumed as “always-on”



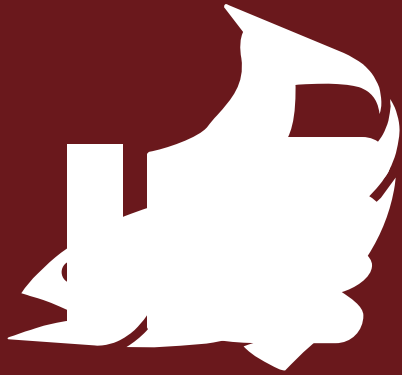


Summary

Summary

- Zero Trust isn't as new as it looks
- However, the technology has changed since the 90s
- Ideally, this technology helps you achieve Zero Trust faster
- My personal opinion:
 - Plan not the whole journey, split it into “agile” portions
 - Focus on topics that create understanding first...
 - ... then on protective & preventative measures ...
 - ... then on detection (usually something with AI & ML & Big-Data)





Don't Panic!

- You made it to the end!
- Raise your hand if you liked this presentation style
- Good luck and thank you for the fish =D

Thanks =)



Chris Trynoga
Senior Solutions Engineer
ctrynoga@akamai.com

Or search “Trynoga” on LinkedIn or Twitter...
... and click on the one who is not a painter!