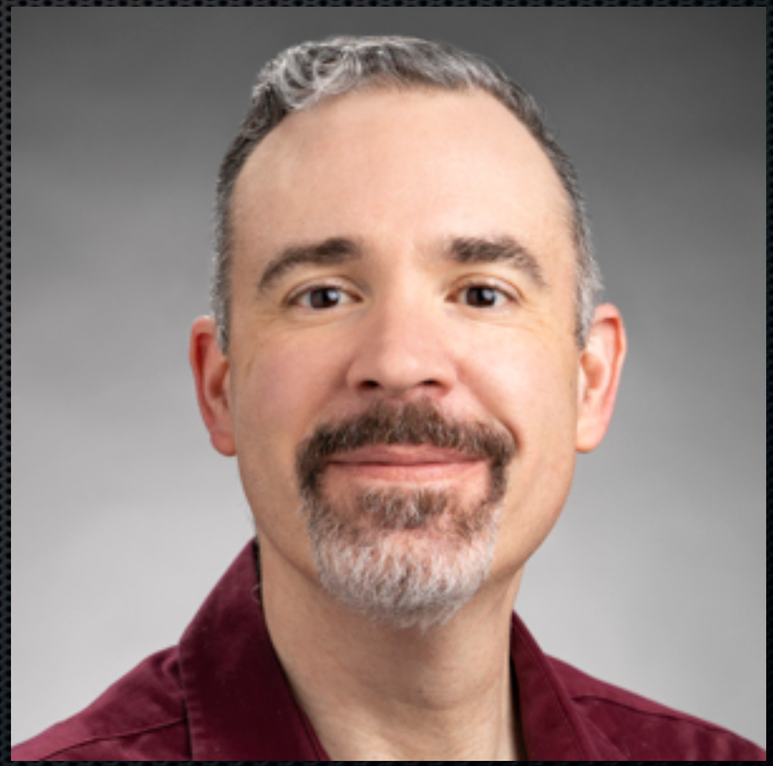
Security by Design: Ideas to keep in mind

2023 MACADMINS CONFERENCE

Who are we?

Ben has been playing with Macs since the mid 1990's, and was thrilled to discover that people would actually pay him for his hobby. He has worked as a consultant and in-house tech in New York City, Connecticut, and the Washington DC area. He is currently getting paid for his hobby by the Johns Hopkins University Applied Physics Laboratory, where he works on making sure the overall Mac experience is as secure and smooth as possible. Since 2015 Ben has focused on cybersecurity and how to balance it with compliance, while working on IT projects to make sure the Mac users are as well taken care of as possible.

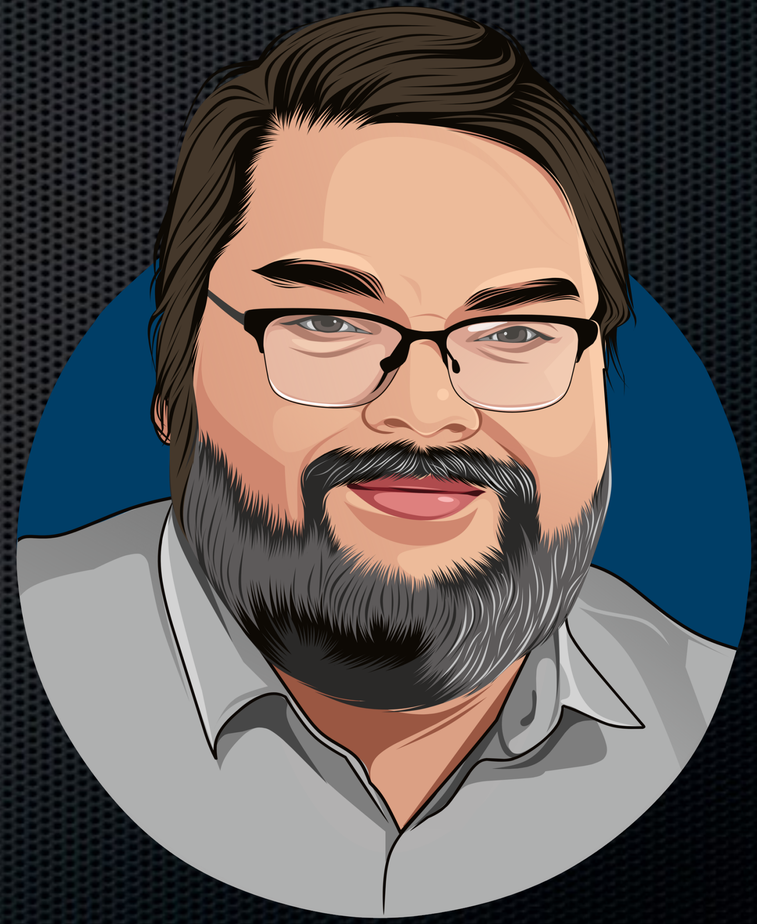


Who are we?

Joe Scalone is a Senior Solutions Architect at Yubico, dedicated to making the internet safer. His main focus is ensuring secure login options are available to everyone. He also assists customers with IAM architectures that provide a roadmap for adoption of modernized authentication. Research, analyze and align specific government regulations with technical partners that are prominent in the public sector to build product specific architectures. He also works with the FIDO Alliance to specify standardized implementations for the FIDO standards.

With over 25 years of experience, Joe has seen IT security shift from usernames to security keys. Recently was at Johns Hopkins Applied Physics Lab as a member of the senior professional staff, as the Technical Manager of Identity and Access Management, Service Manager of Infrastructure Protection and Intern Coordinator for all of internal IT. Previous to that, Joe owned his own IT consulting business where he helped small businesses with anything that was computer related.

Joe lives near Baltimore with his wife and three kids, and loves evangelizing technology to anyone willing to listen. Computer geek, drama geek, food geek, band geek - Joe has a wide range of interests and love of people. He's happiest when assisting people in any aspect, from educating others on unfamiliar technology to volunteering at an animal rescue.



Security By Design: What is it?

Cybersecurity:

The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

-Oxford English Dictionary

Security By Design: What is it?

C I A Triad:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Security By Design: What is it?

CISA

Cybersecurity

Infrastructure

Security

Agency

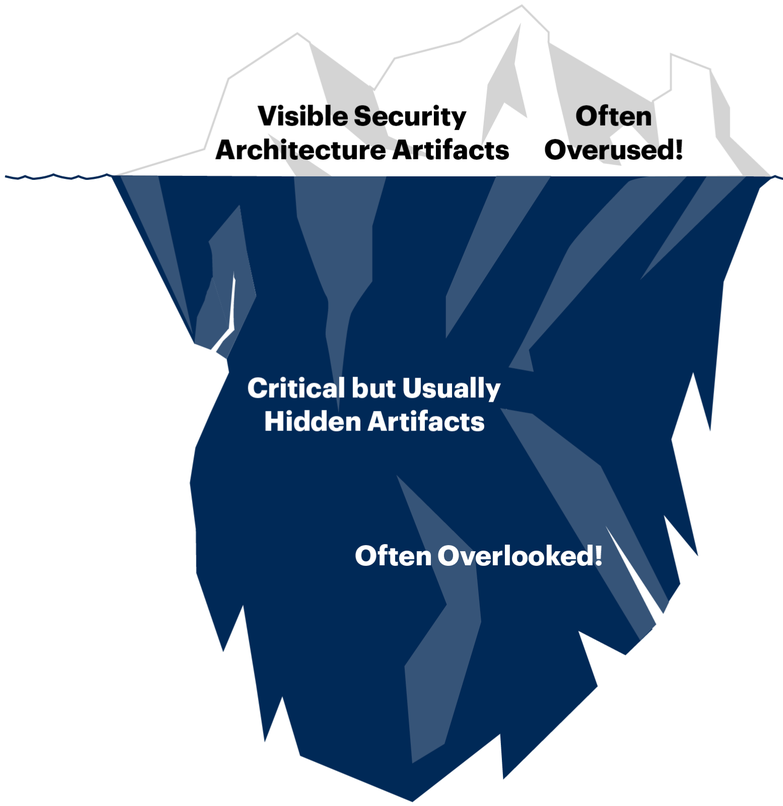
Secure by Design, Secure by Default

Security By Design: Why do we need it?

- It is the right thing to do!
- Contractual Obligations
- Government Regulations
- The design/architectural phases are one of the best times to incorporate security

Security By Design: According to Gartner…

Perceptions of Security Architecture



- Technical Diagrams
- Control Frameworks
- Logical components
- Risk Maps

- Domain Interrelationships
- Trust Relationships
- Data and Information Flows
- Existing Security Controls
- Existing Architecture
- Risk Assessment
- Policy Definitions
- Regulatory Needs
- Strategic Direction
- Business Security Needs

Source: Gartner
778425_C

Security By Design:
How?

Ok, so now what?

Security By Design:
How do we get to How?

ISO 27001 & ISO 27002

PCI DSS

GDPR

FISMA

NIST Cybersecurity Framework (CSF)

Zero Trust

Security By Design:
Zero Trust

What does Zero Trust mean to you?

2023 MACADMINS CONFERENCE

Security By Design:
What does Zero Trust mean to Joe?

- A better way of doing cybersecurity
- Defense in depth taken to 11
- Breaks down silos
- Better utilization of cloud resources

Security By Design:
What does Zero Trust mean to Ben?

- A more complete manifestation of defense in depth
- The next thing in cybersecurity
- A holistic approach to cybersecurity

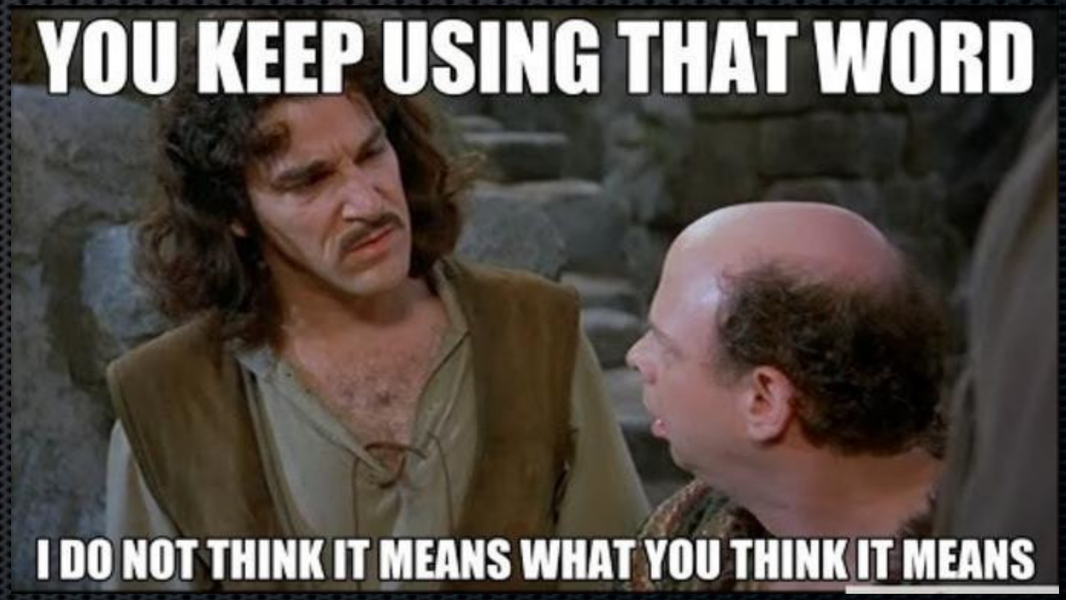
Security By Design: What is Zero Trust?

What it is:

- Philosophy
- Framework
- A long road

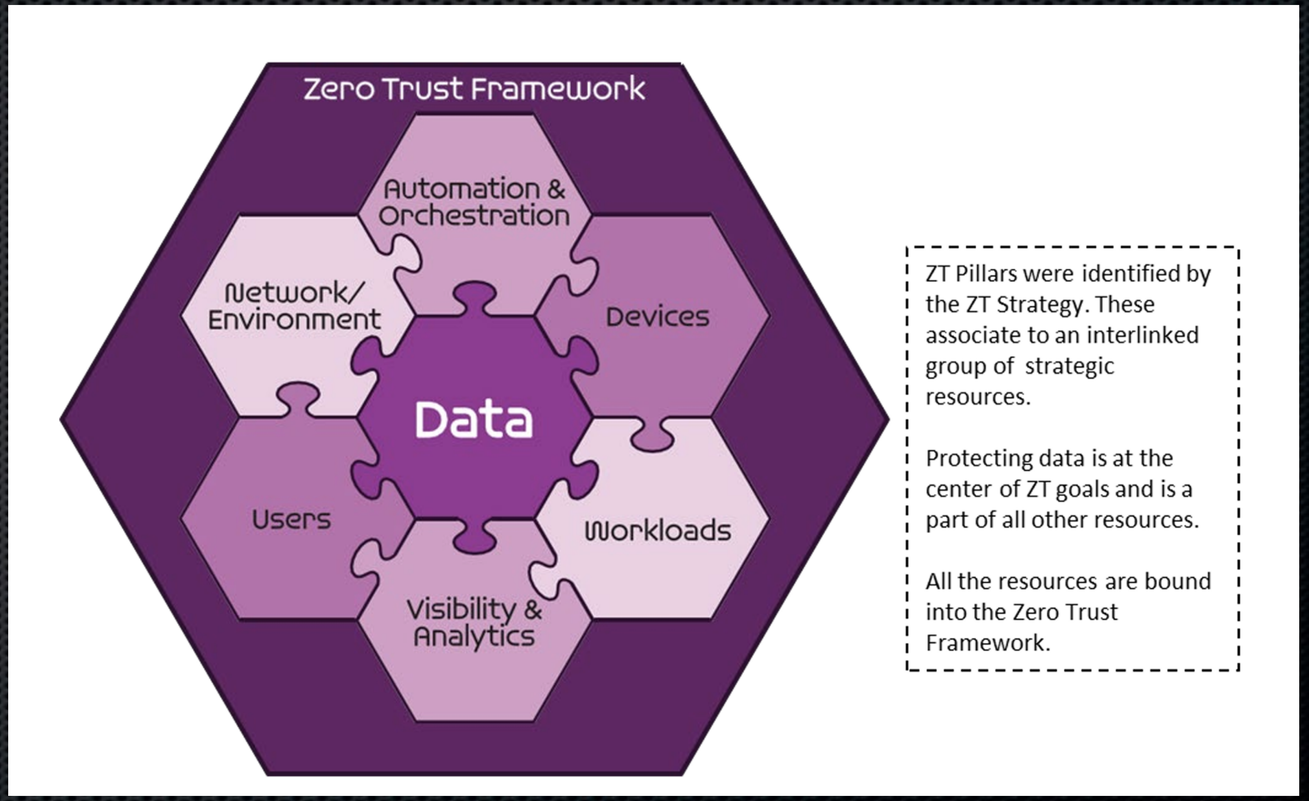
What it is NOT:

- Software
- A quick fix
- Easy



Security By Design: Why Zero Trust?

- Comprehensive
- Data Focused
- Executive Order 14028



Security By Design: Why Zero Trust?

Excerpt from Executive Order 14028:

> The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.
>
> President Joe Biden, May 12, 2021

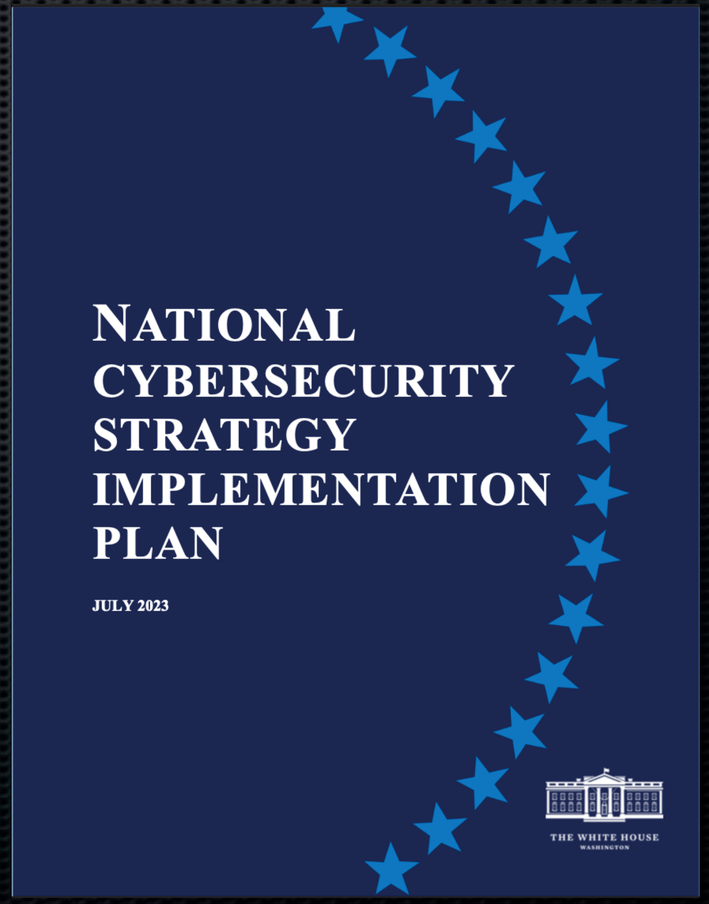
Security By Design: Why Zero Trust?

Excerpt from National Cybersecurity Strategy Implementation Plan:

Initiative Number 1.2.1

> Scale public private partnerships to drive development and adoption of secure by design and secure by default technology.

The Office of the National Cyber Director (ONCD), July 13, 2023



2023 MACADMINS CONFERENCE

@joescalone @benbass #psumac

Security By Design:
7 Zero Trust Pillars

Security By Design: 7 Zero Trust Pillars

1. User

Security By Design: 7 Zero Trust Pillars

1. User
2. Devices

Security By Design:
7 Zero Trust Pillars

1. User
2. Devices
3. Applications & Workloads

2023 MACADMINS CONFERENCE

@joescalone @benbass #psumac

Security By Design:
7 Zero Trust Pillars

1. User
2. Devices
3. Applications & Workloads
4. Data

Security By Design:
7 Zero Trust Pillars

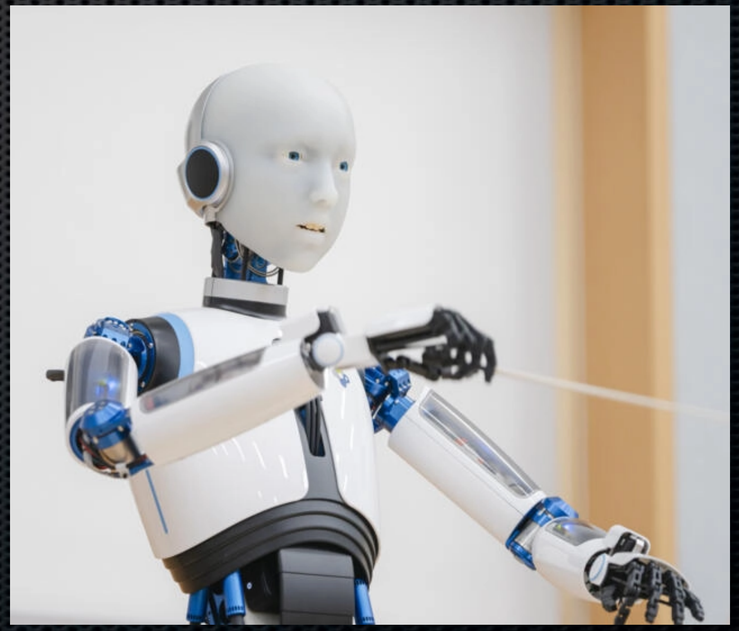
1. User
2. Devices
3. Applications & Workloads
4. Data
5. Network & Environment

2023 MACADMINS CONFERENCE

@joescalone @benbass #psumac

Security By Design:
7 Zero Trust Pillars

1. User
2. Devices
3. Applications & Workloads
4. Data
5. Network & Environment
6. Automation & Orchestration



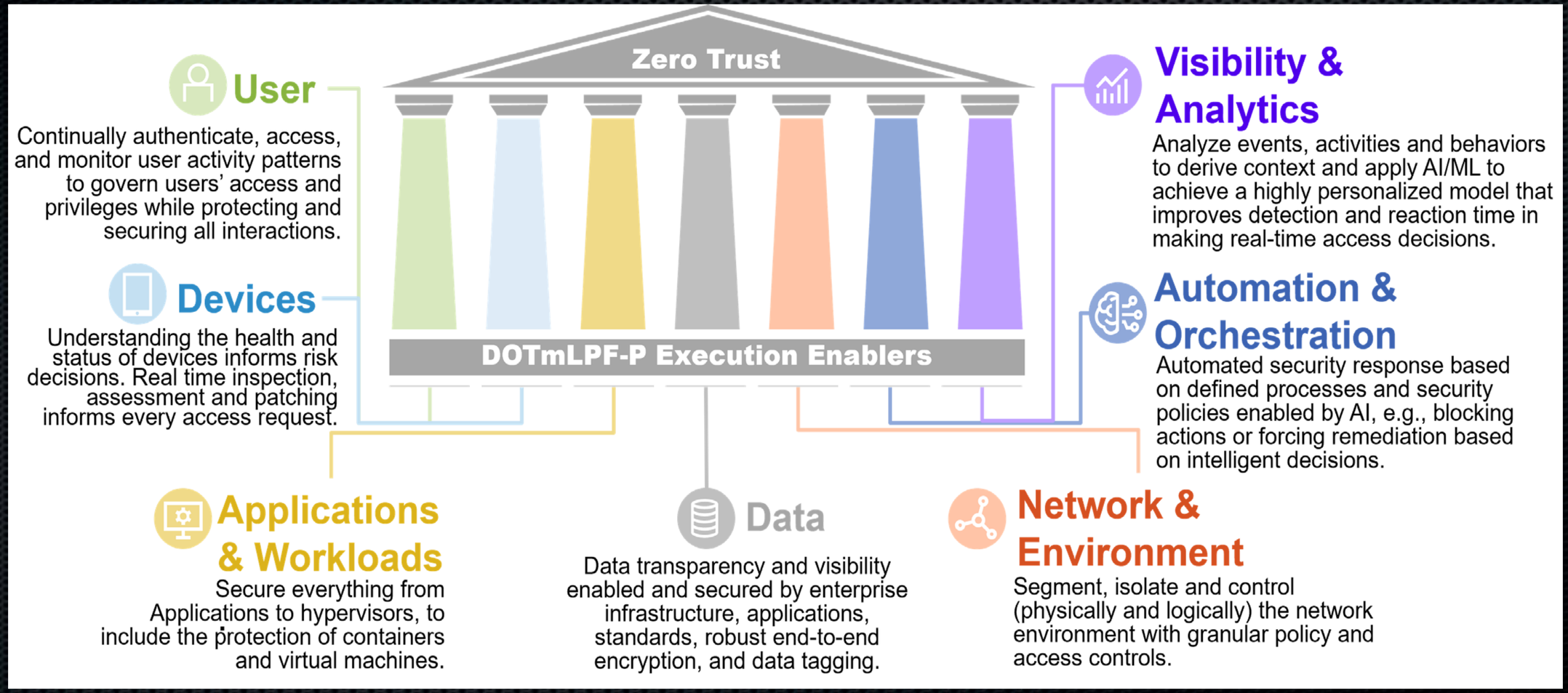
2023 MACADMINS CONFERENCE

Security By Design:
7 Zero Trust Pillars

1. User
2. Devices
3. Applications & Workloads
4. Data
5. Network & Environment
6. Automation & Orchestration
7. Visibility & Analytics

2023 MACADMINS CONFERENCE

Security By Design:
U.S. Dept. of Defense Zero Trust



Security By Design:
7 Zero Trust Pillars

User

- Inventory
- Multi-Factor Authentication
- Identity Federation
- Behavioral
- Continuous Authentication

2023 MACADMINS CONFERENCE

Security By Design:
7 Zero Trust Pillars

Device

- Device Inventory
- Detection and Compliance
- Real time Authorization and Inspection
- Remote Access
- EDR / XDR
  - **E**ndpoint **D**etection and **R**esponse
  - E**X**tended **D**etection & **R**esponse
- Patching
- Unified Endpoint MDM

2023 MACADMINS CONFERENCE

@joescalone @benbass #psumac

Security By Design:
7 Zero Trust Pillars

- Application & Workload
  - Application Inventory
  - Secure Software Development
  - Software Risk Management
  - Resource Authorization & Integration
  - Continuous Monitoring and Authorization

Security By Design:
7 Zero Trust Pillars

Data

- Data Risk Alignment
- Data Governance
- Data Tagging
- Encryption & Rights Management
- Data Loss Protection (DLP)
- Access Controls

2023 MACADMINS CONFERENCE

Security By Design:
7 Zero Trust Pillars

Network & Environment

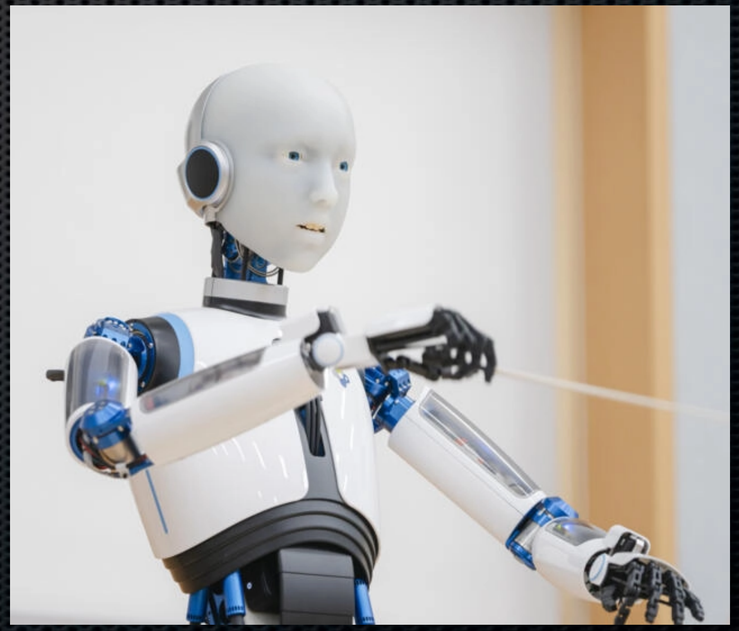
- Data Flow Mapping
- Macro Segmentation
- Software Defined Networking (SDN)
- Micro Segmentation

2023 MACADMINS CONFERENCE

Security By Design:
7 Zero Trust Pillars

Automation & Orchestration

- Policy Decision Point (PDP) & Policy Orchestration
- Critical Process Automation
- Machine Learning / AI
- Security Orchestration, Automation & Response (SOAR)
- API Standardization & Inventory
- Security Operation Center (SOC) & Incident Response (IR)



Security By Design:
7 Zero Trust Pillars

Visibility & Analytics

- Log all of the traffic
- Security Information & Event Management (SIEM)
- Common Security & Risk Analytics
- User & Entity Behavior Analytics (UEBA)
- Threat Intelligence Integration
- Automated Dynamic Policies

2023 MACADMINS CONFERENCE

Security By Design:
7 Zero Trust Pillars

Visibility & Analytics

- Log all of the traffic
- Security Information & Event Management (SIEM)
- Common Security & Risk Analytics
- User & Entity Behavior Analytics (UEBA)
- Threat Intelligence Integration
- Automated Dynamic Policies

2023 MACADMINS CONFERENCE

Security By Design: Conclusion

- Security is incredibly important
- Know what requirements you need to meet
- The best time to incorporate security is at the design/architecture phase
- Data is king
- Zero Trust is a great lens to look through when designing/architecting a system

Questions?

joescalone@gmail.com @joescalone @joescalone joescalone1

ben@benbass.com @benbass @benbass benbasscom

2023 MACADMINS CONFERENCE

Mommas Apple Cake

Ingredients:
3-4 apples, tart
3 T sugar
2 t cinnamon
2 cups sugar
1 cup vegetable oil
4 eggs
1/4 cup orange juice
2 t vanilla
3 cups flour
1 T baking powder
½ t salt

Preparation:
Chop apples in small pieces. Mix 3 tablespoons sugar and cinnamon and set aside. In a large bowl combine sugar and oil. Cream it (mix until fluffy). Add eggs, orange juice and vanilla to the creamed mixture. Add flour, baking powder and salt slowly and beat until smooth. Pour 1/3 of batter into a greased and floured 12-cup bundt pan, alternating with apple mix. Cook at 325F for 60 minutes or until the knife comes out clean. Cool on a rack and sprinkle with confectioner's sugar, or glaze with 1 cup confectioner sugar and 2 – 4 t water. Drizzle over cake. Or just eat without glaze. Freezes well. Great when paired with vanilla or cinnamon ice cream. You can also just eat right off the cooling rack, with your hands! That is what I did as a kid

Potato Pancakes

Ingredients

4 - 5 good sized potatoes with soft or thin skins
1 good sized sweet potato
1 - 2 cups matzoh meal
1 - 2 cups flour
3 - 4 eggs
Roughly 1 teaspoon of salt for every one or two potatoes
Pepper to taste
1 - 2 small or 1 medium onion
Sour Cream. (Amount to taste. I prefer as much as humanly possible. Some say I have a problem. I say, do you want that sour cream?)

Preparation:

Chop the onions and sauté with butter until translucent. Pull from heat and set aside to cool.
Using a hand grater or a food processor, grate the potatoes and alternate layers of potatoes and sweet potatoes, placing all in a single large bowl.
Add salt to the potatoes as they sit. This will draw water from the potatoes, which will soften the sweet potatoes.
Squeeze/drain the mixture of potato and sweet potato. Wring out as much liquid as possible.
Mix in the onions and makes sure they are not hot, as we do not want scrambled eggs.
Add some of the eggs to the Potato mixture, and combine.
Integrate the matzoh meal, then start adding some flour. Add more eggs and or flour until the consistency is correct.
The mixture should stick together and to your hands and come off fairly easily. If it is too wet the mixture will stick to the pan. If the mixture is too dry, the pancakes will taste of too much flour.

Cook the Pancakes:

Place about 1/4" of oil (either olive or canola) in a frying pan/skillet and get the oil hot, be careful of getting the oil too hot.
Put a lump of the potato mixture into the pan and flatten out
Cook until brown and crispy on both sides.
Stack cooked pancake onto cooking pancake, this will allow draining of oil back into the pan.
Place cooked and drained pancakes onto a plate with paper towels to finish draining.
Serve with loads of sour cream (and/or applesauce)

Security By Design: References

CISA Secure By Design
https://www.cisa.gov/securebydesign
DoD Zero Trust Strategy
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
DoD ZT Reference Architecture
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
Gartner Report; Use Security Architecture to Enable "Security by Design"
https://www.gartner.com/document/4352799
NIST SP 800-207, Zero Trust Architecture
https://www.nist.gov/publications/zero-trust-architecture
NIST definition of cybersecurity
https://csrc.nist.gov/glossary/term/cybersecurity
NSA; Embracing a Zero Trust Security Model
https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/
OMB Zero Trust Guidance
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
White House National Cybersecurity Strategy
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
White House Zero Trust Executive Order
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

Security By Design: Resources

Apple Lisa
https://www.macworld.com/article/220228/the-little-known-apple-lisa-five-quirks-and-oddities.html
CIA Triad Image
https://www.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity
CISA Secure By Design
https://www.cisa.gov/securebydesign
Data and Spot
https://treknews.net/2018/08/02/stlv-top-ten-space-animals-star-trek/star-trek-tng-data-spot-cat/
Darth Vader & Luke ZT Meme
https://medium.com/globant/zero-trust-model-beyond-the-perimeter-a4f4a97c7b8c
Eye of Sauron
https://gamerant.com/lord-of-the-rings-eye-sauron-explained/
Executive Order image
https://www.activecyber.net/active-cyber-reviews-executive-order-14028-improving-the-nations-cybersecurity/

Security By Design: Resources

Lan Party
https://arstechnica.com/gaming/2022/11/just-a-bunch-of-idiots-having-fun-a-photo-history-of-the-lan-party/
Robot Conductor
https://www.france24.com/en/live-news/20230630-orchestra-conducting-robot-wows-audience-in-s-korean-capital
User image
https://networknuts.net/user-account-management/
Vim
https://en.wikipedia.org/wiki/Vim_%28text_editor%29
Zero Trust Indigo Montoya Meme
https://www.nccoe.nist.gov/sites/default/files/legacy-files/2_frazier_duo.pdf
Zero Trust Jigsaw puzzle
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf