zentry security

Zero Trust, VPNs, CASB

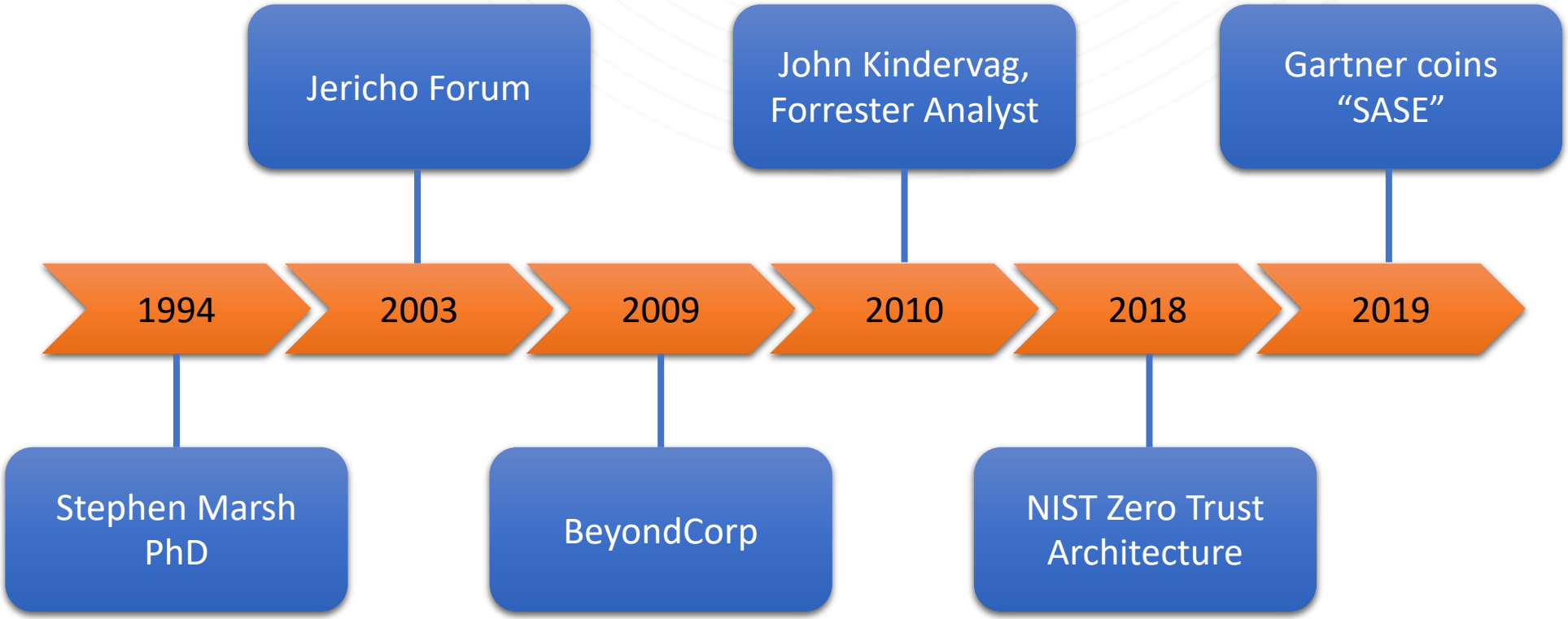
Truth & Hype: Fully Exposed

About me

- Software Engineer turned Product Manager
- Moved to Bozeman, MT during the pandemic
- Two kids, two dogs, two horses, two skis

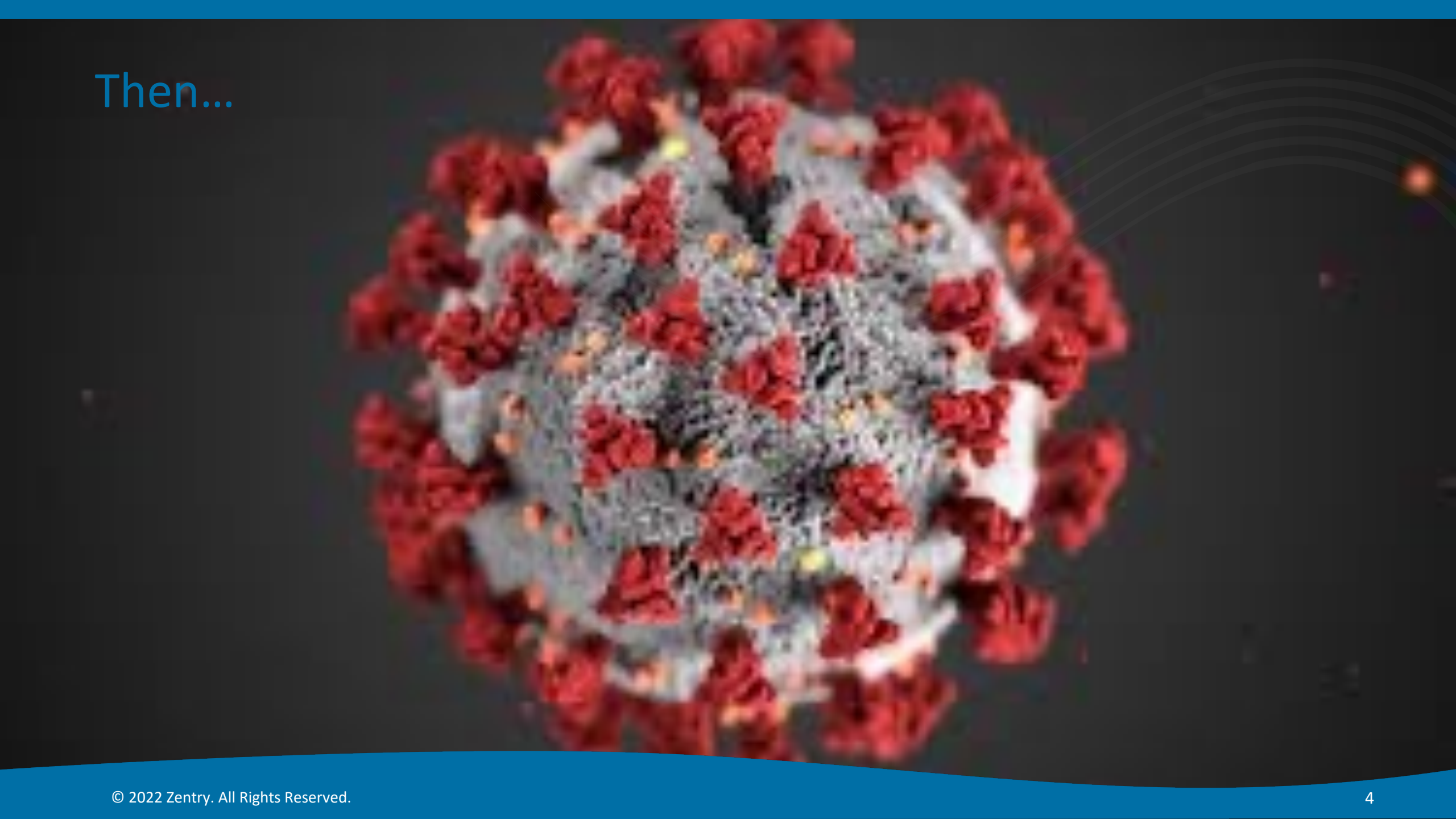
© 2022 Zentry. All Rights Reserved.

The History of Zero Trust



© 2022 Zentry. All Rights Reserved.

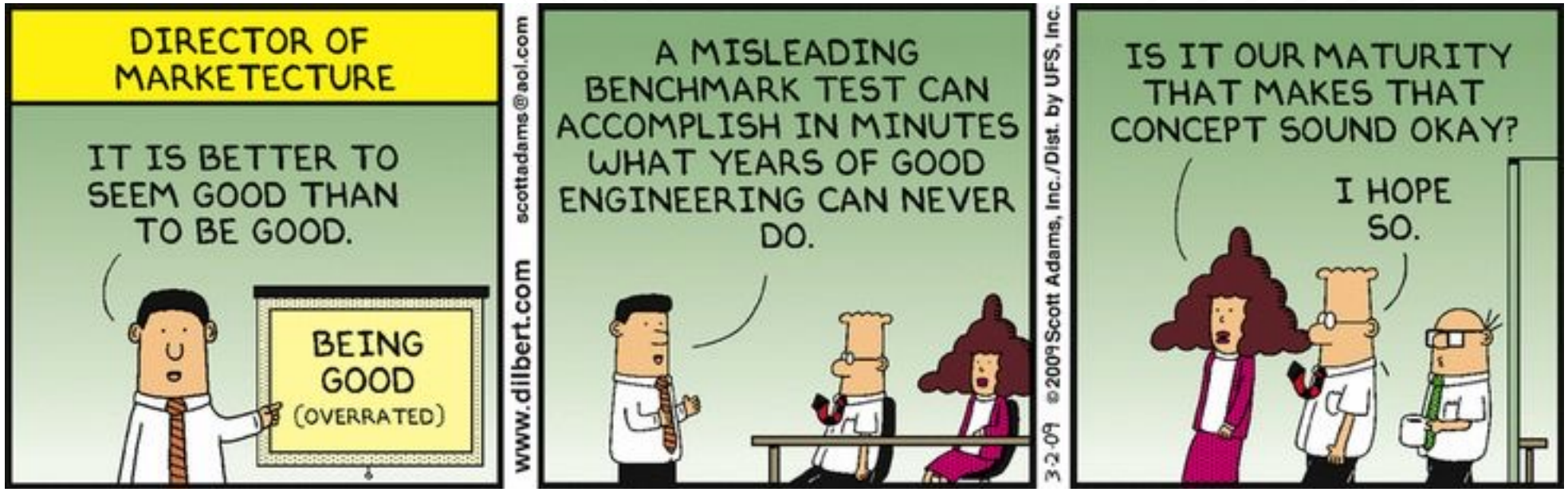
Then…



© 2022 Zentry. All Rights Reserved.

© 2022 Zentry. All Rights Reserved.

Marketing Hype from RSA



In 2022, 26% of RSA Exhibitors claimed the Zero Trust sub-category!

© 2022 Zentry. All Rights Reserved.

Peak of Inflated Expectations…

"Bring Zero Trust Cybersecurity to Connected Buildings"

© 2022 Zentry. All Rights Reserved.

Trough of Disillusionment?

"VPNs Persist Despite Zero-Trust Fervor"

© 2022 Zentry. All Rights Reserved.

Should They Stay or Should They Go?

Advantages

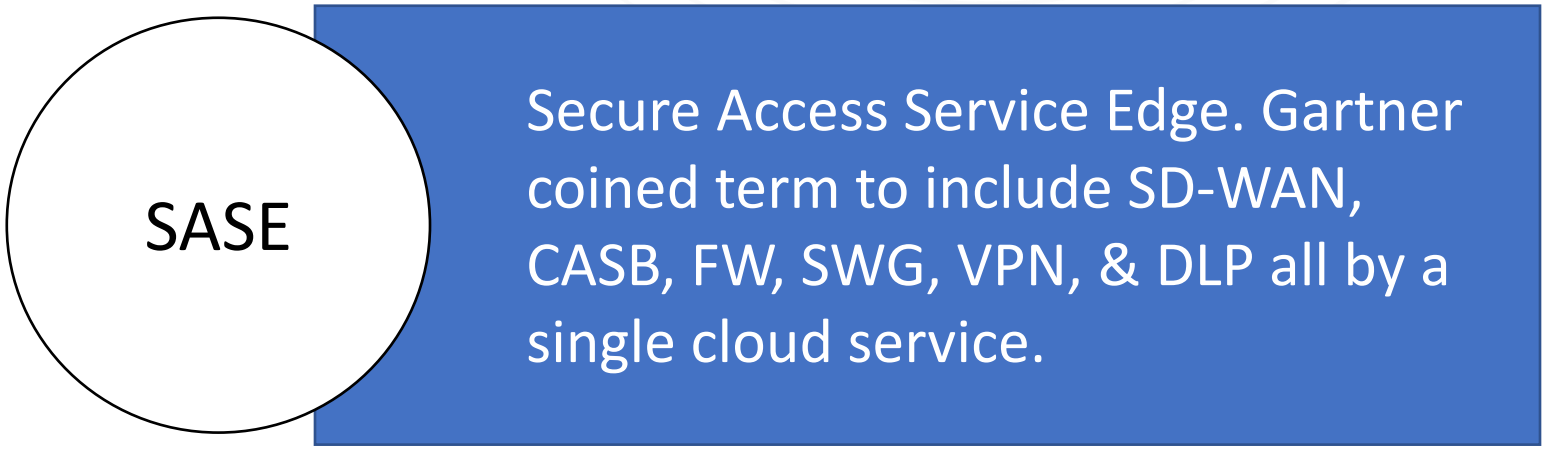
- Mature technology
- You already own them

Disadvantages

- Access over provisioned
- Endpoints in scope
- Hair-pinned Traffic
- Unmanaged Devices

© 2022 Zentry. All Rights Reserved.

Fantasy…



© 2022 Zentry. All Rights Reserved.

to Reality

© 2022 Zentry. All Rights Reserved.

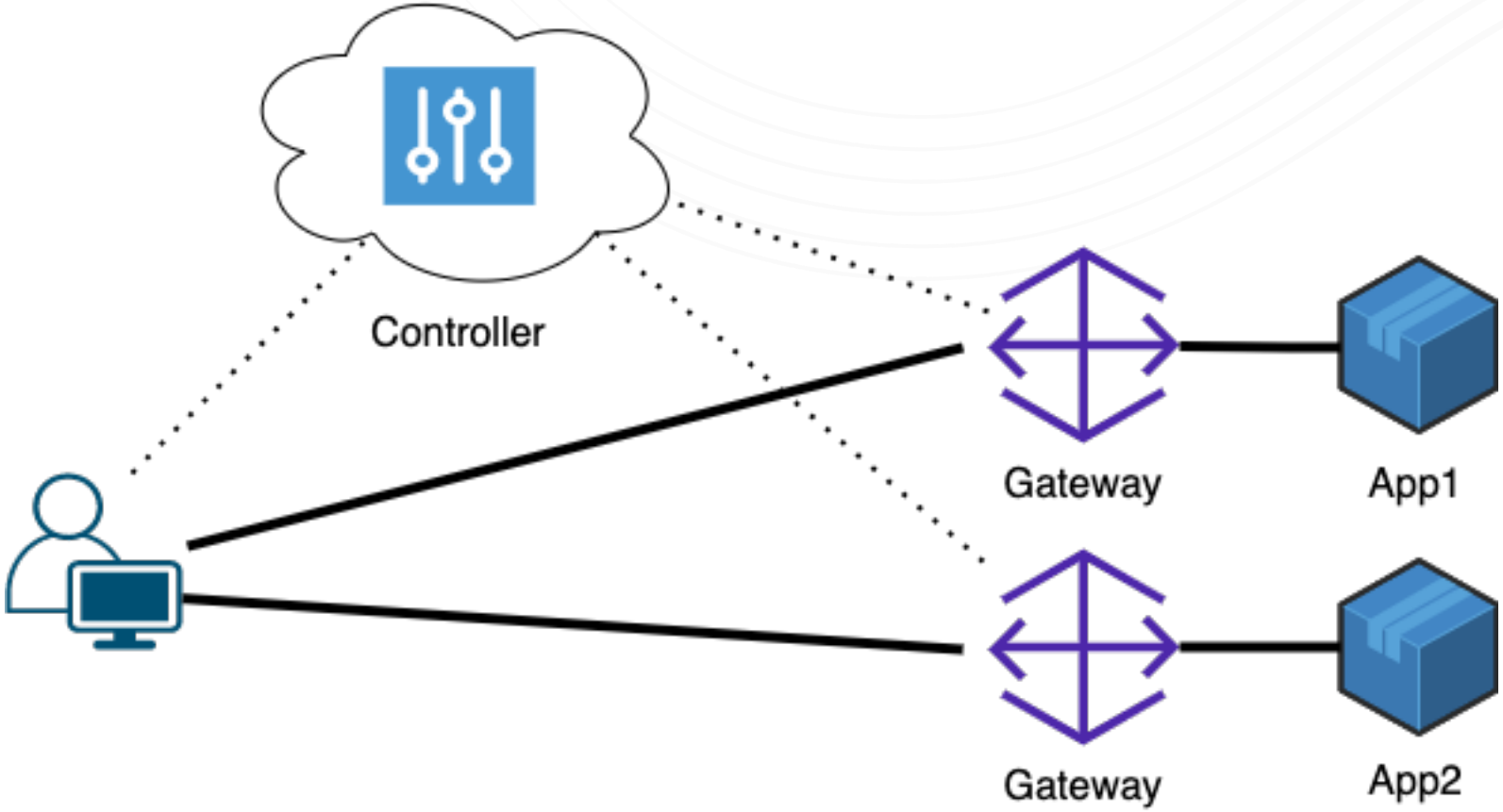
zentry security

Diving Into

Two Approaches to ZTNA

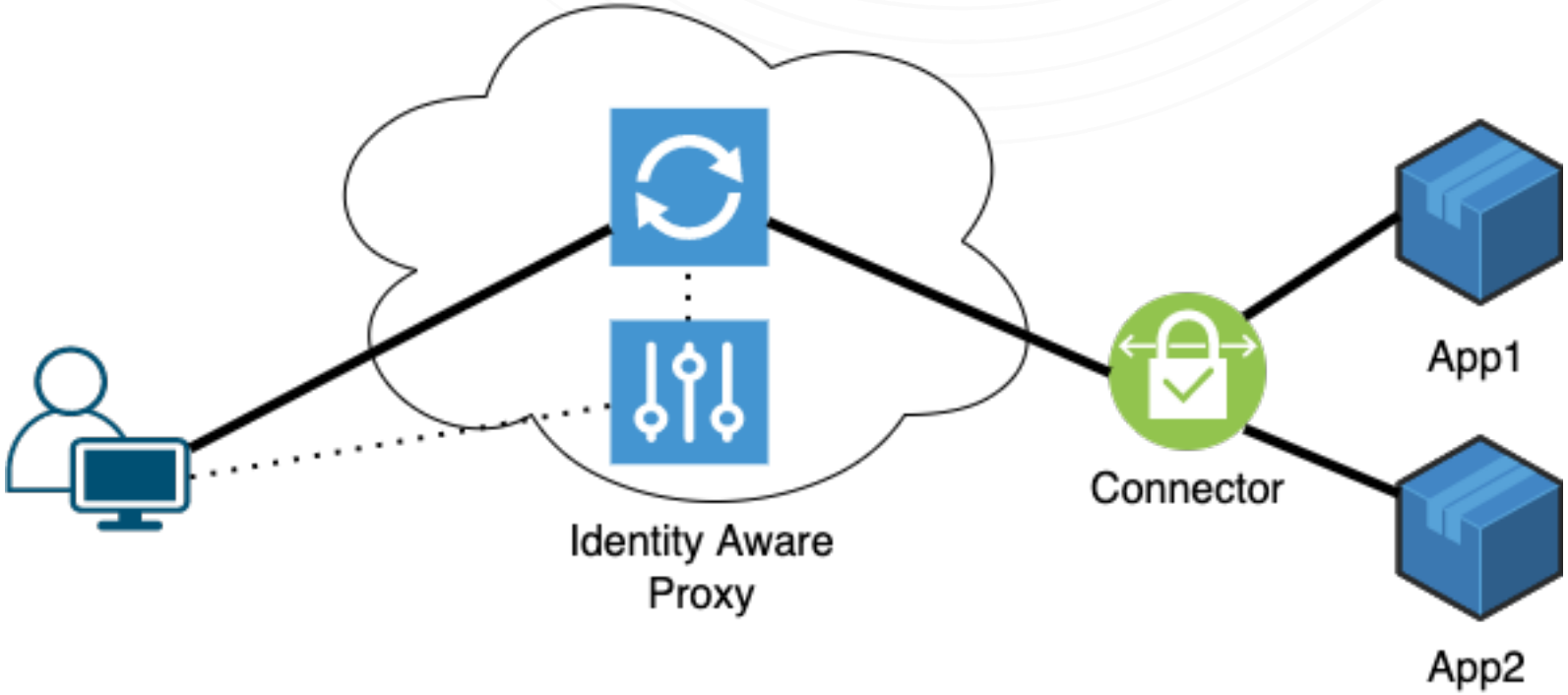
© 2022 Zentry. All Rights Reserved.

Software-Defined Perimeter



© 2022 Zentry. All Rights Reserved.

Identity Aware Proxy



© 2022 Zentry. All Rights Reserved.

Zero Trust Network Access

Summary

	Software Defined Perimeter	Identity Aware Proxy
Advantages	No user-application data transits the provider's cloud	Permits agentless access use cases. Can add value by inspecting data.
Disadvantages	Heavier hosting requirement on your end. Analytics of application data is on you.	User application data transits the provider's cloud.

- ✓ Practice basic security hygiene
- ✓ Identify an urgent business need
- ✓ Select an approach appropriate for your risk tolerance
- ✓ Roll out ZTNA in a phased manner

© 2022 Zentry. All Rights Reserved.

zentry security

Who's not heard of:

Cloud Access Security Broker

© 2022 Zentry. All Rights Reserved.

CASB Lessons Learned

- East-West Data sharing is a real problem
- DLP is hard and requires investment.
  - Have a process in place to deal with incidents
  - Extend where needed for compliance
- Analytics are undervalued
- Encryption at Rest is not a panacea

© 2022 Zentry. All Rights Reserved.

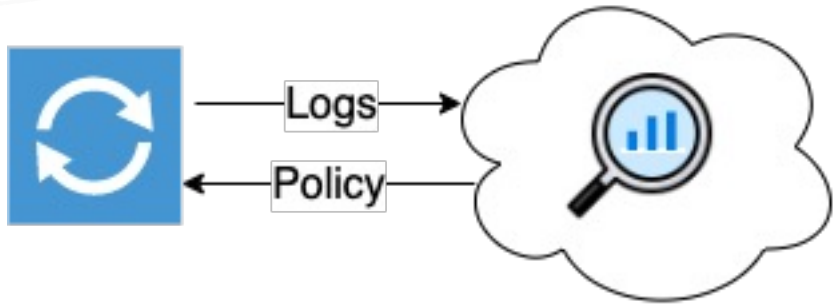
zentry security

Secure Web Gateways

© 2022 Zentry. All Rights Reserved.

Secure Web Gateways

- Enforce HR Policy and Block “bad sites”
- May misclassify certain sites.
  - E.g. ZippyShare and PDF converters
- Recommendations
  - Analyze SWG Logs with CASB Tools
  - Integrate CASB Risk Scores into SWG Policy



© 2022 Zentry. All Rights Reserved.

zentry security

Thank you, ISSA!

© 2022 Zentry. All Rights Reserved.