An Open Standard for Zero Trust Architecture

Altaz Valani
The Open Group
Security Forum Vice-Chair

John Linford
The Open Group Director,
Security Forum & OTTF

About The Open Group

Our Vision:
Boundaryless Information Flow™ achieved through global interoperability in a secure, reliable and timely manner

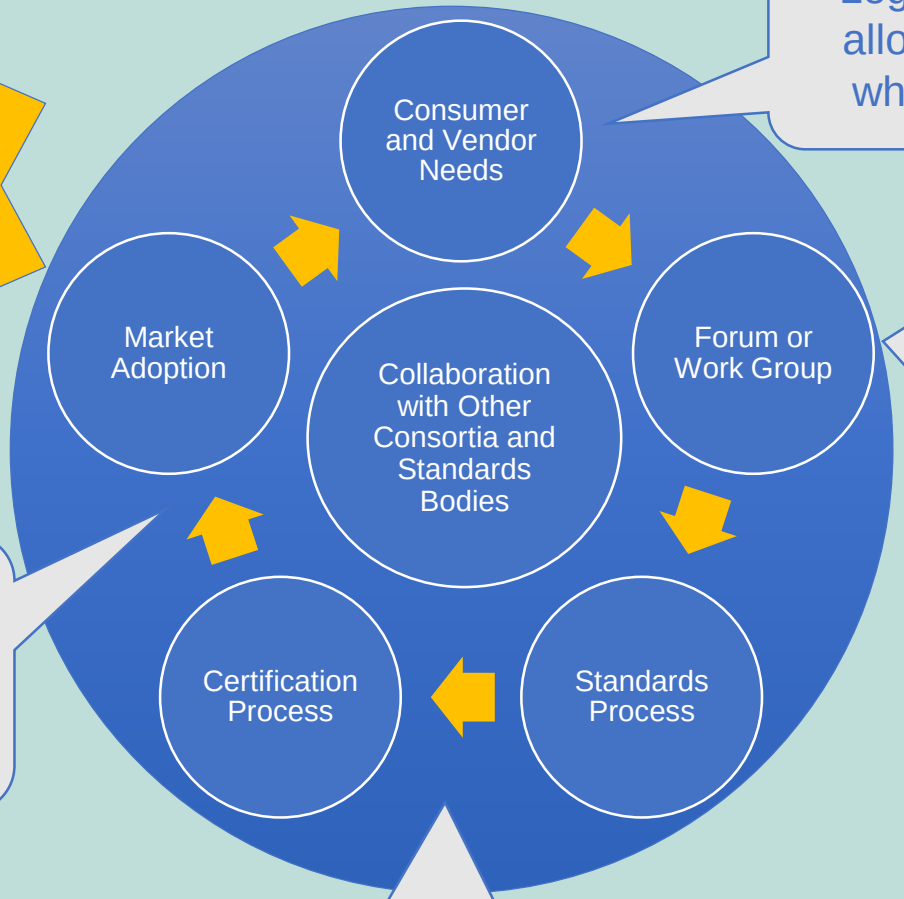
The Open Group is **a global consortium** that enables the achievement of business objectives through technology standards.

With more than 850 member organizations, we have a diverse membership that includes customers, systems and solutions suppliers, tool vendors, and integrators and consultants, as well as academics and researchers across multiple industries.

Making Standards Work®

The Open Group Standards Process
http://www.opengroup.org/standardsprocess/index.html

A proven methodology for initiating new standards activities to meet business objectives and achieve success in the market



Legal & governance structure to allow competitors to collaborate while avoiding anti-trust issues

Open Process Automation™ Forum

Security Forum

OSDU™ Forum

Many major customer organizations, vendors, and governments are existing members operating under The Open Group legal membership agreements

Full lifecycle standards experience, including development of standards, guides, certifications, and open-source code, as well as ecosystem and market development & adoption activities

Open, vendor-neutral standards process

Zero Trust Evolution

2004
Jericho Forum Formally Established

2014
Microsoft Advocates "Assume Breach"

2016
Conditional Access Released

Ongoing
Passwordless Initiative

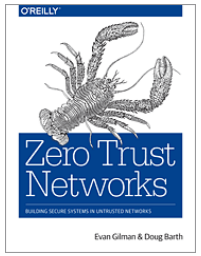
Today

~2004
Network Access Control (NAC) Architectures

2010
Forrester coins "Zero Trust" Term

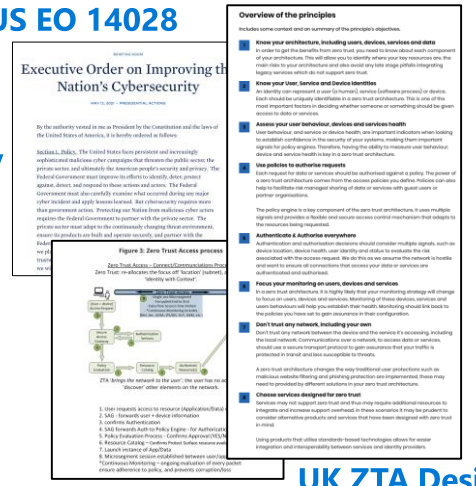
2014
BeyondCorp Published

2017



Government Acknowledgement

US EO 14028



CA Network & Security Strategy

UK ZTA Design Principles

https://www.canada.ca/en/shared-services/corporate/publications/network-security-strategy
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
https://www.ncsc.gov.uk/collection/zero-trust-architecture

Zero Trust & ZTA

Zero Trust - an information security approach that focuses on data/information security, including lifecycle, on any platform or network

Zero Trust Architecture - the implementation of a Zero Trust security strategy that follows well-defined and assured standards, technical patterns, and guidance for organizations

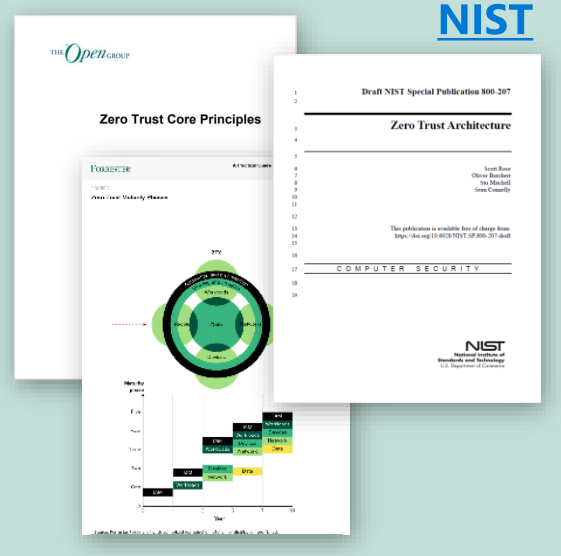
Why do we need Zero Trust?

1. Changing business models and drivers
2. An evolving ecosystem
3. A changing technology landscape
4. Regulatory, geopolitical and cultural forces
5. Disruptive events
6. The shift to remote work and online learning

Zero Trust Today

The Open Group
(Home of the Jericho Forum, TOGAF®, and more)

NIST



Forrester
ZTX Model

Microsoft

1. Growing consensus on strategic nature of ZT
2. Definitions and standards rapidly emerging
3. Key characteristics
   - Asset-Centric and Data-Centric
   - Adaptive access control
   - Holistic across full tech estate (IT, IoT, OT, etc.)
   - Continuous Improvement

Zero ***Assumed*** Trust

Validate Trust Explicitly	Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.

Reduce the Threat Space

- The fewer things there are to protect, or the less the amount spent on their protection, the easier it is to support agility, adaptability, and address disruption and complexity

Reduce the Blast Radius

- Zero Trust expects “assumed compromise”. The ability to localize the compromise reduces the time spent and the cost.

Focus on the Business

Enable Modern Work	Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.
Secure Assets by Value	Security controls shall be designed to protect business assets appropriate to their business value and expected risk.
Implement Asset-Centric Controls	Asset-specific security controls (versus broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.

Make it Easy to do the Right Thing

Enable Pervasive Security	Security discipline shall be integrated into the culture, norms, and processes throughout the organization.
Enable Simple & Sustainable Security	Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.
Utilize Least Privilege	Access to systems and data shall be provided only as required, and access shall be removed when no longer required.

Agile and Adaptive Security

Improve Continuously	Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.
Make Informed Decisions	Security teams shall make informed decisions based on the best information that can be made available.

Zero Trust Commandments

Validate Trust Explicitly	Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.
Enable Modern Work	Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.
Enable Pervasive Security	Security discipline shall be integrated into the culture, norms, and processes throughout the organization.
Secure Assets by Value	Security controls shall be designed to protect business assets appropriate to their business value and expected risk.
Implement Asset-Centric Controls	Asset-specific security controls (versus broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.
Enable Simple & Sustainable Security	Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.
Utilize Least Privilege	Access to systems and data shall be provided only as required, and access shall be removed when no longer required.
Improve Continuously	Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.
Make Informed Decisions	Security teams shall make informed decisions based on the best information that can be made available.

The Commandments are aspirational but provide clarity and guardrails on the Zero Trust journey. They help create a shared vision and shared understanding…

Zero Trust Differentiators

Asset-Centricity

- Digital Era IT enterprises involve data (a primary asset) and those assets that operate or provide output based on that data – apps, APIs, or systems
- OT and IOT assets involve the same 2 genres with nuance

Adaptive Access Control

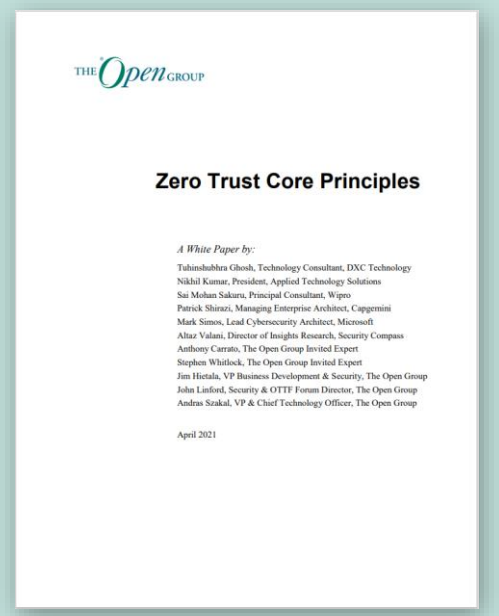
- Agility and adaptability are both dependent on *adaptive access control*, *policy-based administration*, and network granularity (*network of one*)

Data-Centricity

- A subset of asset-centricity, data centricity refers to the shift in data and asset-centricity as opposed to legacy perimeter centricity to meet the drivers of Zero Trust

Current perimeter-centric approaches fail to provide the agility (velocity) and adaptability required by the Digital Enterprise. There is a constant pursuit of solving for the last threat, resulting in an ever-increasing cost that is unsustainable or threat exposure that is crippling.

Zero Trust is on track to a Global Standard


THE Open GROUP

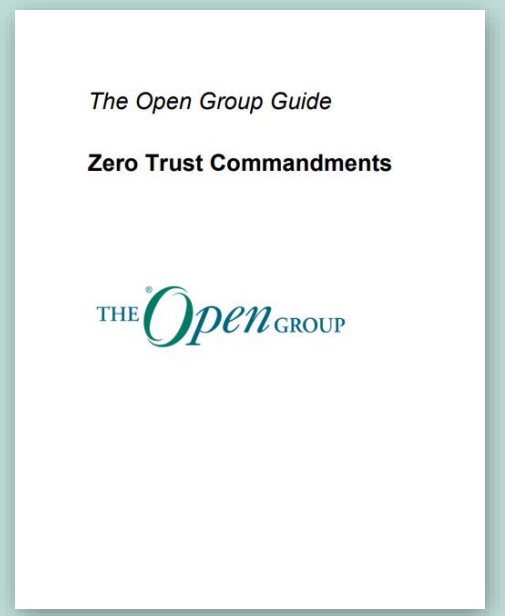
Zero Trust Core Principles

A White Paper by:

Tuhinshubhra Ghosh, Technology Consultant, DXC Technology
Nikhil Kumar, President, Applied Technology Solutions
Sai Mohan Sakuru, Principal Consultant, Wipro
Patrick Shirazi, Managing Enterprise Architect, Capgemini
Mark Simos, Lead Cybersecurity Architect, Microsoft
Altaz Valani, Director of Insights Research, Security Compass
Anthony Carrato, The Open Group Invited Expert
Stephen Whitlock, The Open Group Invited Expert
Jim Hietala, VP Business Development & Security, The Open Group
John Linford, Security & OTTF Forum Director, The Open Group
Andras Szakal, VP & Chief Technology Officer, The Open Group

April 2021

pubs.opengroup.org/security/zero-trust-principles/


The Open Group Guide

Zero Trust Commandments

THE Open GROUP

pubs.opengroup.org/security/zero-trust-commandments/

Zero Trust Reference Model

(Standard being Drafted)

NIST NCCoE is also capturing current state of technology
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Resources

The Open Group

The Open Group Security Forum

Security Forum Publications

- Risk Analysis
- Security Architecture
- Zero Trust
- Data Security
- Information Security Management
- Authentication, Authorization, & Access Management

Zero Trust Publications

- Zero Trust Core Principles White Paper
- Zero Trust Commandments (Guide)
- Zero Trust Commandments (Webinar)

John Linford
The Open Group Director,
Security Forum & OTTF
j.linford@opengroup.org
LinkedIn:
https://www.linkedin.com/in/johndouglaslinford/

Altaz Valani
The Open Group Forum Vice-Chair,
Security Forum
avalani@securitycompass.com
LinkedIn:
https://www.linkedin.com/in/altazvalani/

Thank You!