CSA Zero Trust (ZT)

Working Group Workstream 7 Mini-Charter

Pillar: Data

October 2022

Table of Contents

CSA WORKING GROUP EXECUTIVE OVERVIEW

The goals of the CSA Zero Trust (ZT) Working Group are to

- Collaboratively develop and raise awareness of Zero Trust (ZT) best practices as a modern, necessary, and cloud-appropriate approach to information security (InfoSec).
- Provide thought leadership and educate the industry about the strengths and weaknesses of different ZT approaches so organizations can make informed decisions based on their specific needs and priorities.
- **The scope of Zero Trust research and guidance necessarily includes cloud and on-premises environments along with mobile endpoints and is applicable to the Internet of Things (IoT).**
- **Take a deliberately product and vendor-neutral approach to architectures and implementation approaches for mature Zero Trust implementations.**
- Take technically sound positions on Zero Trust, and make defensible recommendations while remaining product- and vendor-neutral.
- Continue to advocate for, and enhance Software-Defined Perimeter (SDP) as a proven architecture to achieve some of the key principles and benefits of Zero Trust, particularly in the network space.

Overall Working Group Scope and Responsibilities

The working group advocates and promotes the adoption of Zero Trust security principles, developing and providing practical and technically sound, vendor-neutral guidance and thought leadership on how organizations can and should approach Zero Trust implementations for their cloud and on-premises environments, along with mobile endpoints. This group will build on and leverage established and recognized Zero Trust frameworks and controls.

Link to overall workgroup charter: CSA Zero Trust Working Group Charter 2022 - Final V1

Overall Working Group Vision

This working group aims to educate, develop and promote best practices, and advance Zero Trust standards by fostering a culture of collaboration between relevant organizations to achieve consistent and effective Zero Trust practices in and for cloud, hybrid and mobile endpoint environments and with IoT applicability. Key focus areas of this working group include:

- Educate practitioners on current and future Identity trends as they relate to Zero Trust
- Promote the usage and advancement of Identity standards and best practices
- Describe the state of (the "as-is") cloud ZT
- Promote interoperability between legacy on-premise and cloud-hosted ZT systems, and the applications they protect
- Guide the transition from legacy and siloed security to a modern cloud and hybrid ZT, to help organizations overcome their network, security, operational and identity challenges
- Assist with the pursuit of compliance to established standards (e.g. IETF, NIST, CISA)
- Document and promote the standardization and usage of emergent technologies and ZT-appropriate terminology
- Assist with ZT architecture (ZTA), adoption, deployment best practices, and guidelines
- Collaboratively describe how related research areas (such as IAM) integrate with a Zero Trust strategy (with a focus on asset security)

ZT Working Group Structure and Workstreams Scope

Given the broad scope and complexity of Zero Trust the overall CSA ZT research working group will be broken out into the following nine workstreams to facilitate parallel research and development efforts.

1. Zero Trust as a Philosophy & Guiding Principles

2. Zero Trust Organizational Strategy & Governance

3. Pillar: Identity
4. Pillar: Device
5. Pillar: Network/Environment
6. Pillar: Applications & Workload
7. Pillar: Data
8. Automation, orchestration, visibility & analytics
9. Zero Trust Architecture, Implementation and Maturity Model

Several of these workstream topics are interrelated and could potentially be tackled in an integrated manner by a single sub-workgroup where appropriate.

Workstreams

The initial scope and activities for each work stream are described in the following subsections.

The scope, activities and specific deliverables will be defined and refined by each workstream workgroup in their own mini-charter document during their initial stages of operation. *(Content pertaining to other unrelated workstreams can be deleted.)*

The initial draft mini-charters will be presented for CSA ZT Leadership Team review and approval, followed by CSA Executive Steering Committee review.

1. Zero Trust as a Philosophy & Guiding Principles

2. Zero Trust Organizational Strategy & Governance

3. Pillar: Identity

4. Pillar: Device

5. Pillar: Network/Environment

6. Pillar: Applications & Workload

7. Pillar: Data

The US Department of Defense Zero Trust Reference Architecture states that Zero Trust protects critical data, assets, applications and services. A clear understanding of an organization's data, applications, assets and services is critical for a successful implementation of a Zero Trust architecture. Organizations need to categorize their data, applications, assets and services in terms of mission criticality and use this information to develop a comprehensive data management strategy as part of their overall Zero Trust approach. This can be achieved through the categorization of data, developing schemas, and encrypting data at rest, in transit and in use. Solutions such as DRM, DLP, Software Defined Storage and granular data-tagging are relevant in protecting critical data.

Data needs cross functional integration with governance, applications/workload, network and identity. It also needs integration with maturity model.

Integration points with pillar2: governance, pillar 6: applications / workload pillar and 5: network, pillar 2: identity workstream 9: maturity model will need to be worked out.

Data should be protected at rest, in applications, on endpoint devices, and in transit over networks. Scope of data protection should include confidentiality, integrity and availability. Businesses should inventory, categorize, label data, protect data at rest and in transit, and deploy mechanisms for detecting data exfiltration and protecting high risk data in use. Zero-Trust creates a more “data-centric” and risk-based approach to cybersecurity, in which companies should begin to identify, categorize and inventory data assets immediately, prioritizing deploying data protections for the most critical, high value data assets.

This workstream will focus on defining, exploring, and documenting the requirements, implications, architectures, and technologies associated with data security in Zero Trust environments. Work will include exploring and evaluating Zero Trust Data Protection (ZTDP) mechanisms. It may also examine how Zero Trust architectures change how organizations approach data security.

8. Automation, orchestration, visibility & analytics

9. Zero Trust Architecture, Implementation and Maturity Model

Workstream Activities and Deliverables

The working group has a primary objective to develop, publish and actively disseminate valuable and actionable research, targeting information security practitioners, leaders, and influencers. Given the scope and complexity of the topic and the high level of interest

Given the scope, complexity and high level of demand for ZT guidance and training the working group will need to adopt agile and incremental approaches for defining and developing workgroup deliverables.

Overall working group and individual workstream deliverables and supporting activities will include the following:

1. **CSA ZT Research Workstream Group Kick-off package**
    a. Draft Mini-Charter

b. Kickoff meeting slide deck
c. Meeting Invitation & agenda
d. Call(s) for workstream volunteer participation
    i. Leaders & co-chairs
    ii. Research working group participants
    iii. Lead authors

2. **Research documentation and publications**
   - a. Specifications
   - **b. Architectural guidance**
   - c. Technical documents
   - **d. Thought leadership articles (blogs, newsletters & Circle posts)**
   - **e. Position papers**
   - f. Implementation guidance
   - g. **Recorded panel discussions** for open house/drop-in calls
     - i. With some post-event editing and narration as appropriate
3. Engineering solutions:
   - a. Security of data in use (data masking, encryption, truncation)
   - b. Security of data at rest (data masking, encryption, truncation)
   - c. Data loss prevention (SQL proxy)
   - d. Use cases for legacy solutions, private cloud versus public cloud, risk based solutions
4. narrative
5. Polls and questionnaires
6. Training Materials
7. Supporting materials such as:
   - **a. Presentations**
   - **b. Blog posts**
   - **c. Webcasts**
   - d. Recommendations for and inputs to CSA training materials to be developed

Deliverables will be governed by CSA's intellectual property rights policy.

Working Group Organization, Membership and Management

The working group will be composed of CSA volunteers and staff. The working group is chaired by appointed co-chairs and comprises representatives from cloud computing industries and information security professions.

Principal attendees will be designated representatives from an entity and any alternate may be designated by each principal.

The co-chairs and workstream leads may appoint others as necessary to assure the effective execution of the defined work.

Others individuals may be invited to attend meetings by the principals as deemed necessary to provide inputs to topics under discussion.

All working group members should have or create accounts on the CSA Circle and subscribe to and participate freely in the CSA ZT Circle Community.

Volunteer Responsibilities and Recognition

Responsibilities and expectations for CSA volunteers are addressed in the Volunteer FAQ on our website. Detailed volunteer expectations tend to be addressed project by project when someone steps up to contribute to a specific workstream or document. For Zero Trust working groups regular and sustained participation is expected.

Authors of CSA documents are recognized on the download page of the document(s) they contribute to (e.g. Critical Controls Implementation for Oracle Fusion Applications). The CSA also has two awards/formal recognitions which can be found on the website (details below). We're hoping to expand this further in the future.

- Ron Knode Award - Analysts nominate particularly dedicated volunteers and the staff votes for 2 people from each region (Americas, APAC, EMEA). This is awarded annually

- Research Fellow - Volunteers nominate themselves after 100 hours of volunteering with CSA and contributing to one or more research papers. Acceptance is rolling.

ZT Working Group Leadership Team

There is an overall CSA Zero Trust research leadership group composed of CSA leadership, workgroup co-chairs, ZT research workstream leaders, and selected recognized industry ZT subject matter expert advisors (SMEs). Other individuals may be invited to attend leadership meetings by the principals as deemed necessary to provide inputs to topics under discussion.

Workstream Co-Leads

The overall ZT working group and the work stream sub-groups will be led by qualified, experienced co-chairs and workstream leads selected by CSA leadership. The ZT working group co-chairs will assist with the leadership responsibility of the working group. Workstream co-chairs may enlist others as necessary to assure the effective execution of the defined research. The respective co-chairs will be identified promptly as each group is launched.

Workstream Workgroups and Leadership

Workstream workgroups shall be led by one or more co-leads who shall report directly to the main working group and the ZT Leadership Team of which they will be a part.

It is recommended that co-leads plan to allocate at least 6-8 hours per month to dedicate to the workstream working group. This is to provide time to attend essential working group and leadership meetings, coordinate with other working group co-chairs on relevant initiatives and review evolving workstream content and delverables.

In addition to the designated work streams additional standing or ad hoc sub-work groups composed of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main workstream working group co-chairs and the overall ZT Leadership Team.

Workstream Leadership Duties

- Prepare agendas for meetings/calls.
- Record and/or publish minutes for each workstream call.
- Coordinate with DCSA leadership and support to document and maintain workstream artifacts such as workstream mini-charters, deliverable descriptions, etc.
- Delegate responsibilities to working group members, including Lead Authors.
- Use the working group mandate and objectives to guide the work of the working group.
- Involve all members in the decision making.
- Keep a written track of working group activities.
- Schedule deliverables and set milestones towards completion of deliverables.
- Draft proposed resolutions (motions) for inclusion in written reports
- Orchestrate contributions to the produced working group documents by different volunteers
- Judge items in or out of scope for the Group.
- Revises deliverables timeline as needed.
- Stay up-to-date with all phases of a policy proposal relevant to the WG

Lead Authors

Each ZT workgroup and workstream delliverable shall have one or more Lead Authors. It is recommended that Lead AUthors allocate at least 4-6 hours per month to dedicate to the working group. This is to provide time to attend essential subgroup meetings, and lead the efforts developing materials documenting industry best practices and guidance.

Authors Duties

- Work with other lead authors and working group leadership to formulate the scope, objectives and high level structure of research initiatives and deliverables.
- Contribute your expertise to the whitepapers under your care, both directly as an author and indirectly through guiding other volunteer efforts.
- Prepare updates for the rest of the working group on initiative status once per month.

Subcommittees

The ZT working group Leadership Team and Workstream Co-Leads may designate and organize other standing or ad-hoc subcommittees to aid in research and collaboration pertaining to Zero Trust. Such sub-working groups shall report directly to the overall ZT Leadership group and shall collaborate with the applicable workstream working groups.

Collaboration with Other CSA Groups & Initiatives

The working group or specific workstream work groups may also collaborate and implement resource sharing between cloud communities and other CSA (or external) working groups such as the following to facilitate knowledge sharing and the timely completion of deliverables and activities needed to support or enable the working group's defined body of work. The working group will share research and standards that align with other CSA Working Groups, advisory groups, existing CSA research and industry partners (i.e SDOs, gov) such as the following.

- IAM - Identity
- IoT - Device
- SDP - Network
- Enterprise Architecture
- Cloud Key Management
- Data Security & DLP

Hybrid and Multi-cloud are also related topics since many ZT implementations are or will be multi-cloud and similarly many cloud customers will need to have hybrid implementations. SDP is a discrete yet still highly relevant ZT implementation option.

- Hybrid Cloud Security Working Group | CSA (cloudsecurityalliance.org)
- Multi Cloud Security | CSA (cloudsecurityalliance.org)

Appendix

Mini-Charter Revision History

10/6/2022	Initial template created for each workstream co-leads to customize and refine for CSA ZT Leadership Team review and approval, followed by CSA Executive Steering Committee.	Erik Johnson