Cloud Security Alliance
SDP and Zero Trust Working Group

Foundation For Zero Trust
Quarterly Update - October 13, 2021

Agenda

CSA Announcements
Introduction of SDP and Zero Trust Working Group leadership team
Overview and history of SDP and Zero Trust
Current Threat Landscape
Risk Analysis for effective ZTA Strategy
The Future of SDP and Zero Trust.
Ongoing Work : Ideas, and How You Can Help

Cloud Security Alliance CSA

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and organizations that offer qualified professional services based on CSA best practices.

In 2009, CSA released the Security Guidance for Critical Areas of Focus In Cloud Computing, providing a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. The following year, CSA launched the industry's first cloud security user certification, the Certificate of Cloud Security Knowledge (CCSK), the benchmark for professional competency in cloud computing security, along with the Cloud Controls Matrix (CCM), the world's only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations. By way of follow up, in 2015 together with (ISC)², CSA debuted the Certified Cloud Security Professional (CCSP) certification, representing the advanced skills required to secure the cloud.

CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA research prides itself on vendor neutrality, agility and integrity of results. CSA has a presence in every continent except Antarctica. With our own offices, partnerships, member organizations and chapters, there are always CSA experts near you. CSA holds dozens of high quality educational events around the world and online. Please check out our events page for more information.

Working Groups (WGs)

The CSA maintains Working Groups across 36 domains of Cloud Security. Some WGs are dormant

Big Data	Blockchain/Distributed Ledger	Cloud Component Specifications
Cloud Controls Matrix	Cloud Data Center Security	Cloud Data Governance
Cloud Security Services Management	Cloud Vulnerabilities	CloudAudit
CloudCISC	CloudTrust	CloudTrust Protocol
Consensus Assessments	Containers and Microservices	Enterprise Architecture
Enterprise Resource Planning (ERP) Security	Financial Services Stakeholder Platform	Health Information Management
Incident Management and Forensics	Industrial Control Systems (ICS) Security	Innovation
Internet of Things	Legal	Mobile
Mobile Application Security Testing (MAST)	Open API	Open Certification Framework (OCF)
Privacy Level Agreement	Quantum-safe Security	SaaS Governance
Security as a Service	Security Guidance	Software Defined Perimeter and Zero Trust
Telecom	Top Threats	Virtualization

Leadership Team

SDP Co-Chairs

Bob Flores
Jason Garbis
Junaid Islam

SDP Technical Advisor

**Juanita Koilpillai*

CSA Research Analyst

Shamun Mahmud

Overview and history of SDP and Zero Trust

- The original Zero Trust was developed by the US Intelligence Community 35 years ago to support counter terror operations
- ZT was briefly revitalized as Black Core for the NetCentric Warfare program in 2002 using Mobile IPv6 clients
- The current ZT was a collaboration between US IC and the vendor community that replaced Mobile IPv6 with SDP

Overview and history of SDP and Zero Trust

- Forrester's John Kindervag builds upon the USG's DoD/IC Zero Trust initiatives (aimed at mainstream commercial applications)
- Google BeyondCorp (Commercial viability in action)
- Federal (USG) Zero Trust Initiatives (CSA responses)
  - Zero Trust Strategy
  - Zero Trust Maturity Model
  - Technical Reference Architecture

Current Threat Landscape

Risk Analysis for ZTA Strategy

Future of SDP (and Zero Trust)

- The future is bright...Zero Trust is the current major trend in the security industry
  - US Federal Government - mandatory adoption of ZT Architectures: President Biden's Executive Order in May 2021
  - Private Sector Momentum
  - Broad Vendor Support
- Wide participation in technical Working Groups and Standards Committee around Zero Trust
- SDP is a well-proven architecture for achieving Zero Trust
  - Ongoing enterprise adoption and vendor support
- This Working Group is helping advance the state of the art
  - Best Practices
  - Use Cases
  - Broadening its applicability

SDP Working Group Deliverables: Historical and In-Progress

Historical

- SDP Glossary v2.0. Q2 2018
- SDP Architecture Guide Q1 2019
- SDP Adoption and Awareness Poll Q2 2019
- SDP as a DDoS Preventive Mechanism. Q3 2019
- SDP and Zero Trust Whitepaper Q2 2020
- Zero Trust Architectures - Training Course - Date TBD

In Progress

- Integrating SDP and DNS for enhanced Zero Trust policy enforcement - Whitepaper - completing Peer Review - Q4 2021
- SDP Specification v2.0 - in Peer Review : *Q4 2021*

SDP WG - ideas for initiatives

- SPA Everywhere / SPA for IoT
  - Whitepaper, open source toolkit and initiative
- 5G and ZT (and SDP) - Smart Cities
  - Whitepaper on SDP architectures for 5G
- SDP ZT POC in lab
  - As outlined in the ZT whitepaper
- SDP and DNS Integrations: POC in lab
  - Demonstrating ideas fro the new whitepaper
- Zero Trust Policy Model - ideas for whitepaper / lab
- Identity Management and Zero Trust
- Microsegmentation
- Using Zero Trust to Protect Legacy Applications
- Zero Trust adoption survey
- SDP Case Studies / business benefits
- integration with Endpoint Management systems - whitepaper / POC
- Cloud segmentation

Lots of ideas...your opportunity to contribute!

Join the SDP and Zero Trust Working Group

The SDP Zero Trust working group launched with the goal to develop a solution to stop network attacks against application infrastructure. With the adoption of cloud services the threat of network attacks against application infrastructure increases since servers can not be protected with traditional perimeter defense techniques. This is where SDP comes in. Join now and see why SDP truly is the optimal engine for Zero Trust

CSA Working Groups are the go-to source for best practices, research and tools for providing security assurance and privacy in the cloud. CSA's diverse membership of industry practitioners and corporate members has converged and continuously cycled through researching, analyzing, formulating and delivering arguably the most advanced research and tools available across the cloud security spectrum.

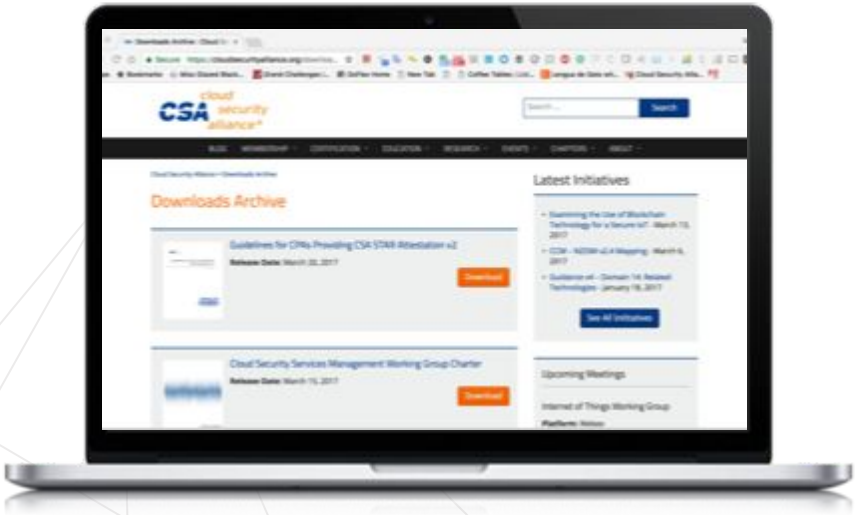
Next SDP ZT WG Meetings

Working Session: Next Initiative Planning

Wednesday, November 3rd, 4pm ET / 1pm PT

SDP and Zero Trust WG: Quarterly Update

Wednesday, January 12th, 4pm ET / 1pm PT



Contact CSA Research

Email: research@cloudsecurityalliance.org

Twitter: @CloudSA

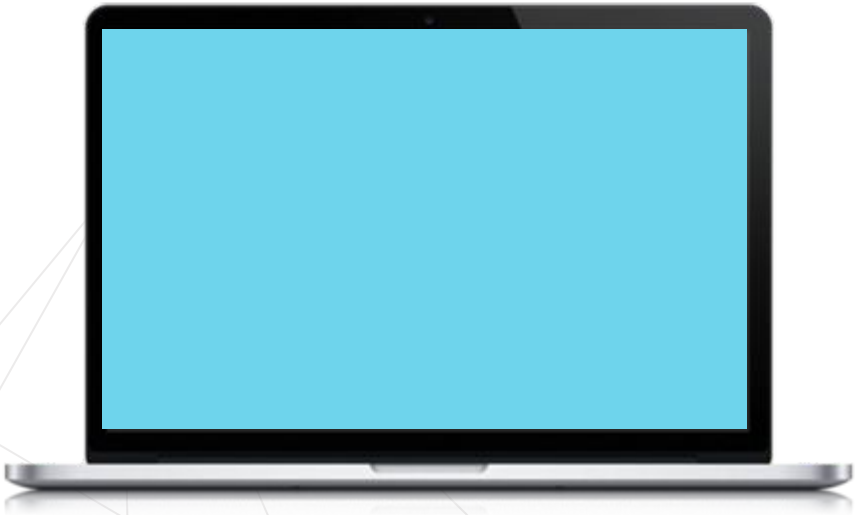
Overview: www.cloudsecurityalliance.org/research

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

Supplemental slides

Additional topics (TBD)

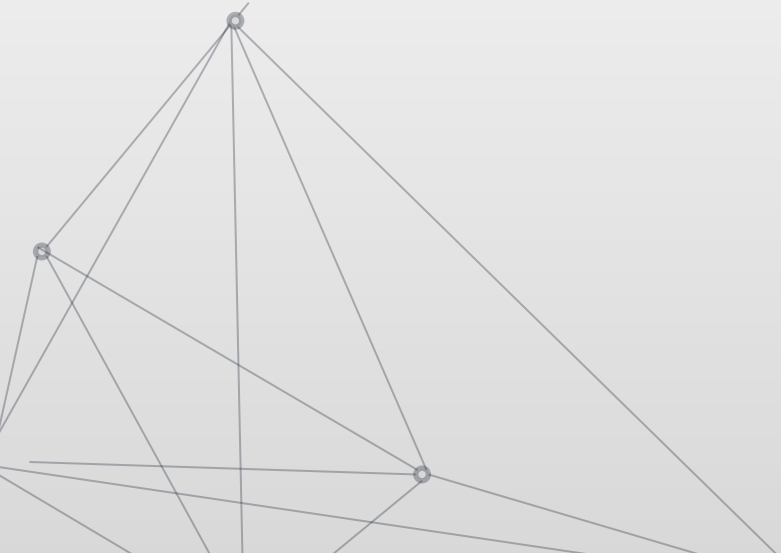


SDP Working Group Initiatives solicited

Status: Ongoing.

1) Call for Topics

1) **Objective:** Research future areas where SDP could help. Should be aimed at reinforcing Zero Trust security postures. Filter to a reference implementation
2) **Application:** POCs and Use cases.



Let's skip this slide - we need to talk through the concept of briefings, and only advertise ones that we have ready to deliver.

SDP Working Group

Status: Ongoing. Briefings: Currently Available

1) Open Source DDoS Initiative

1) **Objective:** Research SDP as a high speed Internet-based packet filter
2) **Application:** Enable access to mission critical sites during DDoS attacks

Zero Trust - some milestones