



Securing Sovereign and Global Clouds

Jim Reavis, Chief Executive Officer

ABOUT THE CLOUD SECURITY ALLIANCE

“To promote the use of best practices for providing security assurance within Cloud Computing and provide education on the uses of Cloud Computing to help secure all other forms of computing.”



Building security best practices for next generation IT



Global, not-for-profit organization



Research and Educational Programs



Cloud Provider Certification



User Certification



The globally authoritative source for Trust in the Cloud

165k+
INDIVIDUAL MEMBERS

100+
CHAPTERS

2009
CSA FOUNDED

500+
CORPORATE MEMBERS

35+
ACTIVE WORKING GROUPS

SEATTLE/BELLINGHAM// GLOBAL
HEADQUARTERS

2,000+
STAR REGISTRY
ENTRIES

12,000+
CONTRIBUTING RESEARCH
VOLUNTEERS

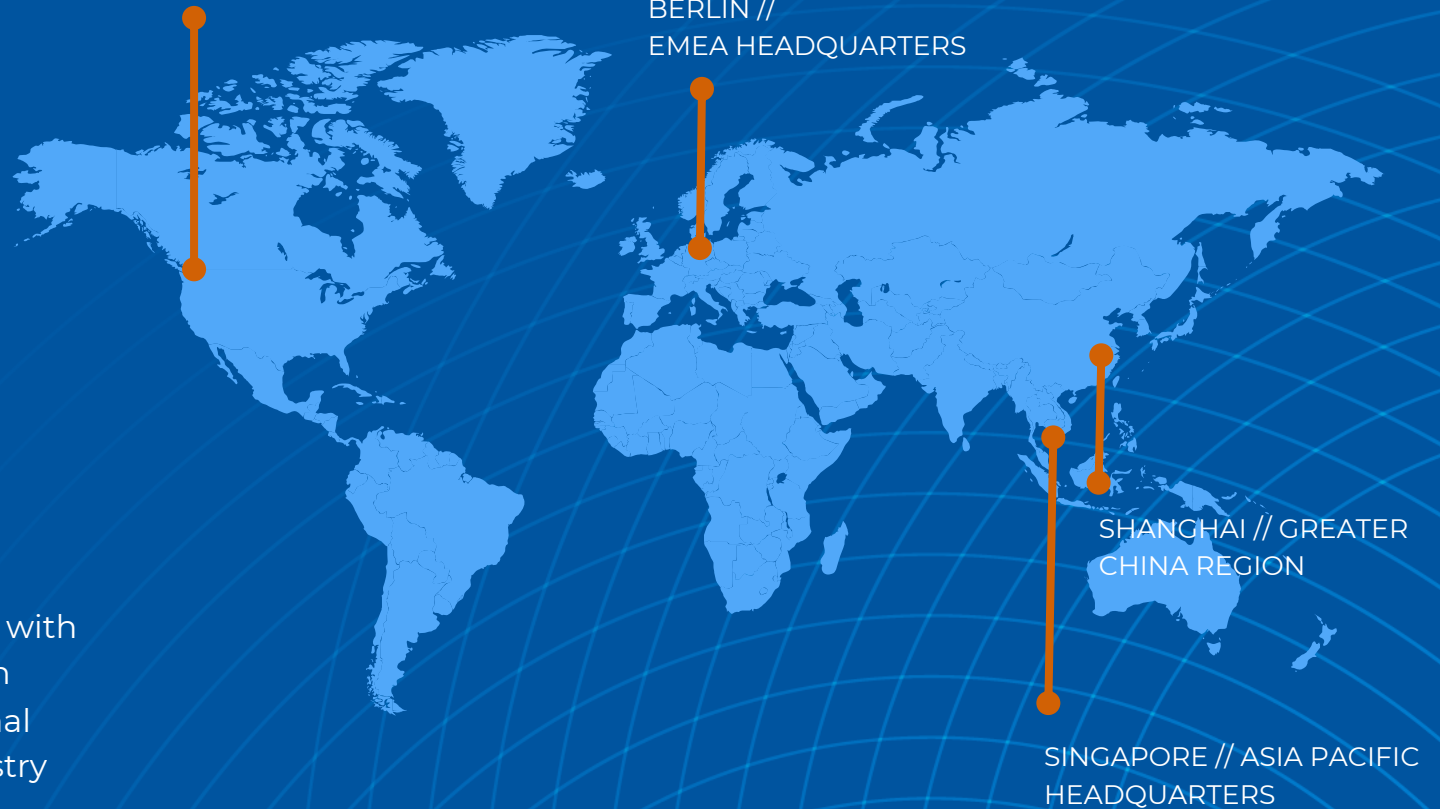
BERLIN //
EMEA HEADQUARTERS



CSA research is
FREE! 500+
Publications



Strategic partnerships with
governments, research
institutions, professional
associations and industry



Key Trends

- Zero Trust
- Automation
- Containers & serverless
- Multi-cloud
- Edge computing
- Resilience
- SaaS security
- Confidential computing
- Passwordless
- ChatGPT & other AI/ML
- Cloud supply chain
- Assurance
- Cloud native security
- Threat modeling
- Quantum
- Vulnerability tracking
- CSP Change Control Notification
- Data sovereignty

Sovereign, Regional Cloud Examples

- Google Cloud Platform Germany (partnership with Deutsche Telekom)
- AWS GovCloud (US Federal Government)
- Singapore: Microsoft and HTX (Home Team Science and Technology Agency)
- China Aliyun
- Gaia-X: infrastructure for Europe
- Balancing national interests vs broader technology innovation

Optimizing Sovereign Clouds

- Benefits
 - Compliance with national data protection interests
 - In-country data center infrastructure
- Drawbacks
 - Less technological innovations
 - Weaker resilience
- Aligning Sovereign with Global Clouds
 - Shared administrative models
 - Improved data management & security technologies

Generalized Cloud Security concerns from Enterprise CISOs

- Global optimization & standardization VS regional & nation-state priorities
- Effective realization of the shared responsibility model
- Compliance regimen
- Data protection, resilience, managing complexities
- Evolving threat vectors
- Security at scale: automation, orchestration
- Cloud security workforce readiness

CISO Expectations of Major CSPs

- Looking for CSP leadership in addressing:
 - Cyber risk and board visibility
 - Threats to critical infrastructure and ransomware threat vectors
 - Threat intelligence sharing with competitors and tenants
 - Reasonable compatibility with competitors
 - Software sourcing and provenance, SBOM, API security
 - Cyber skills development and talent development
 - Harmonization of global compliance requirements
 - Confidential computing accessibility

Key Survey Recap



Surveys Referenced

<https://cloudsecurityalliance.org/artifacts/cloud-security-and-technology-maturity-survey/>

<https://cloudsecurityalliance.org/research/topics/top-threats/>

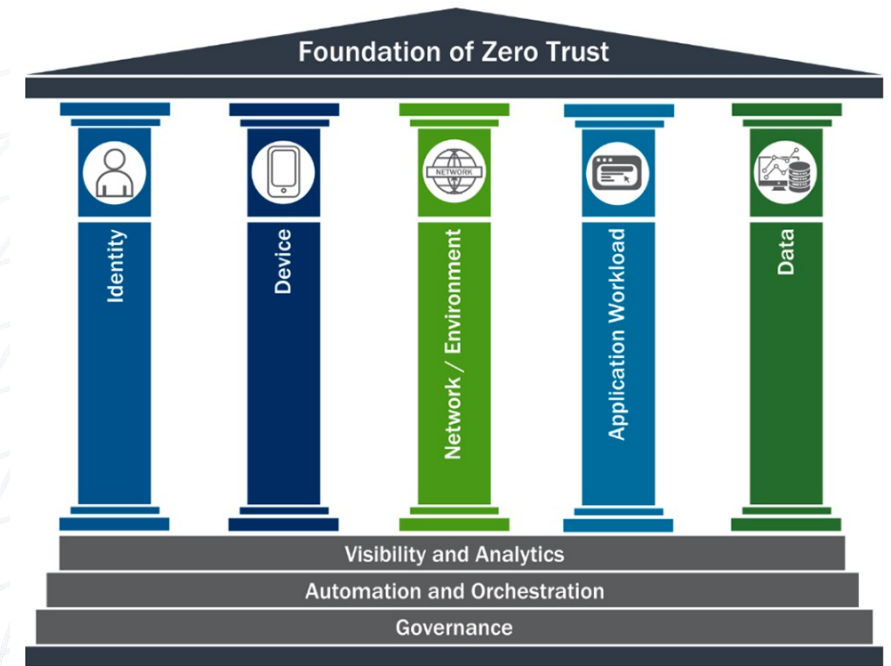
<https://cloudsecurityalliance.org/artifacts/ciso-perspectives-and-progress-in-deploying-zero-trust>

<https://cloudsecurityalliance.org/artifacts/measuring-risk-and-risk-governance/>

<https://cloudsecurityalliance.org/artifacts/data-loss-prevention-and-data-security-survey-report>

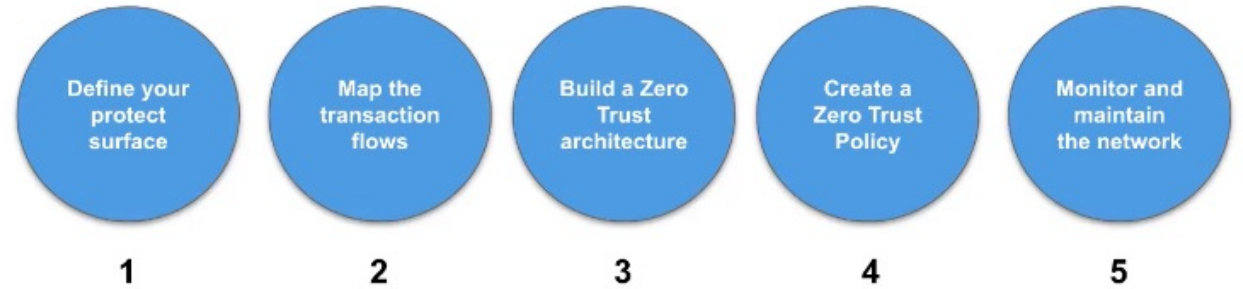
- Security & Technology Maturity
 - Crown Jewel Data ↑
 - Multi-Cloud ↑
 - Automation ↑
- Top Threats to Cloud Computing
 - All Tenant-based in top 11
- Zero Trust
 - Priority for 75% of CISOs
- Measuring Risk & Risk Governance
 - Manual estimation of cloud usage
 - Lack of post-procurement assurance
 - Infrequent adjustment of risk metrics
- Data Loss Prevention & Security
 - Cloud is #1 Data sharing mechanism
 - Legacy DLP too complex, needs modernization

- Center is positioning Zero Trust as “Philosophy informing Strategy”
 - Assume everything can be compromised
 - Protect assets with least privilege access
 - Identity as a foundation
 - Continuous verification
- Training, Research, Resource Hub

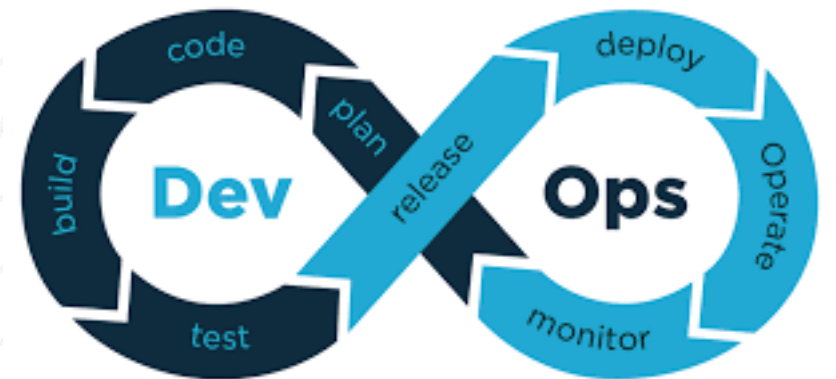


- www.cloudsecurityalliance.org/zt

- Use 5 Step Methodology
- Extend 5 Pillars to “Cloud Native”



- DevOps > DevSecOps
- Container and Serverless deployment
- Focus on Automation & Tooling
- Align Microservices Architecture with Zero Trust Network Architecture
- Layer 7 Access Control
- Infrastructure as Code
- Policy as Code





OpenAI / ChatGPT

- AI as a Service: biggest game changer since the cloud
- OpenAI has significant lead over other Large Language Models (LLM)
- First CSA guidance paper released at RSA: *Security Implications of ChatGPT*
- Four Dimensions
 1. How malicious actors can use it to create new and improved cyberattacks
 2. How defenders can use it to improve cybersecurity programs
 3. How it can be directly attacked to produce incorrect or otherwise bad results
 4. How to enable the business to use it securely and responsibly

Free Research to improve

Top Downloads

- CCM & CAIQ
- Security Guidance
- Top Threats
- DevSecOps
- Enterprise Architecture V2
- Cloud Threat Modeling
- Cloud Incident Response Framework
- SaaS Governance
- Serverless / Containers
- IoT Controls Framework



Architectures and Components

Cloud Component Specifications
Cloud Security Services Management
Enterprise Architecture
Hybrid Cloud Security



Assessments and Audits

CAIQ
Cloud Controls Matrix
Continuous Auditing
Open Certification Framework
Privacy



C-Level Guidance

CxO Trust
Security Guidance
Standards



Emerging Technologies

Artificial Intelligence
Blockchain
High Performance Computing
Industrial Control Systems
Internet of Things
Quantum-safe Security



Industry Specific

Financial Services
Health Information Management



Securing DevOps

Application Containers and Microservices
DevSecOps
Serverless



Security Services

Cloud Key Management
Enterprise Resource Planning
Identity and Access Management
SaaS Governance
Security as a Service
Software-Defined Perimeter
Zero Trust



Threat Intelligence

Cloud Incident Response
Global Security Database (GSD)
Top Threats
Vulnerabilities

Keys to a Secure & Sovereign Future

- ✓ Shared Responsibility & Fate
- ✓ Transparency
- ✓ Innovation
- ✓ Policy
- ✓ People

Thank You!

CSA *cloud
security
alliance*®

jreavis@cloudsecurityalliance.org
www.cloudsecurityalliance.org