State of the Cloud
Strategy & Innovation

Jim Reavis, Chief Executive Officer
Cloud Security Alliance
www.cloudsecurityalliance.org

Cloud fast becoming the Primary IT system

- Gartner
  - Public cloud growing at least 18% in 2021
  - 70% of orgs increasing cloud spending due to COVID-19 disruptions
  - SaaS largest component
- Cloud Security Alliance
  - Over 50% of orgs running 40%+ workloads in public clouds (up from 25% in 2019)
  - 67% are multi-cloud
- CSO Magazine
  - 45% say teams' skill gaps are major cloud security challenge
- 3-6 million unfilled cybersecurity jobs

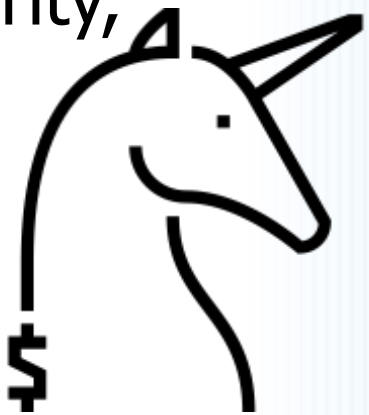
Gartner Cloud Forecast (8/2/2021)

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2020	2021	2022
Cloud Business Process Services (BPaaS)	46,066	51,027	55,538
Cloud Application Infrastructure Services (PaaS)	58,917	80,002	100,636
Cloud Application Services (SaaS)	120,686	145,509	171,915
Cloud Management and Security Services	22,664	25,987	29,736
Cloud System Infrastructure Services (IaaS)	64,286	91,543	121,620
Desktop as a Service (DaaS)	1,235	2,079	2,710
Total Market	**313,853**	**396,147**	**482,155**

Cloud Security As Foundation Of Cybersecurity

- Hastened by the pandemic, organizations adopt virtual or "hybrid virtual" model
- Cloud provides uniform leverage point for securing cloud as well as on-premise assets, remote devices – "hybrid virtual"
- Cloud "Security as a Service" facilitates on-demand security, when and where you need it
- Valuations of public and private cloud security companies exceed other cybersecurity companies



Cloud & Cybersecurity Trends

- Cloud Native
- Multi-cloud
- Sovereign Cloud (e.g. GAIA-X)
- Artificial Intelligence as a Service
- Vertical Cloud
- Cloud + 5G
- Serverless vs Containers
- Software Defined Organizations
- Automation
- Data Growth vs Privacy
- Attack Economics & Sophistication
- Zero Trust
- Cybersecurity is National Security
- Blockchain
- Next Gen Cloud Hopper Attacks
- Compliance as Code
- Ransomware > Extortionware
- Quantum Resilience
- Immutable Storage
- Multi-Factor Authentication Everywhere

So, is the cloud secure?

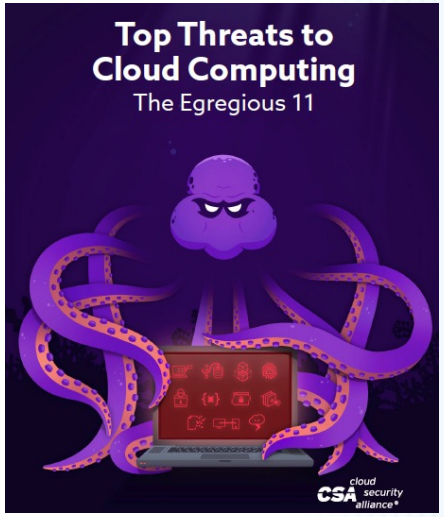
- Cloud, like other forms of technology, can achieve an acceptable level of security with the appropriate investment and application of best practices
- Majority opinion is that cloud is probably more secure than traditional on-premise:
  - Tier 1 cloud providers have invested heavily into security
  - Cloud operating models put constraints on what users are allowed to do
- The security challenge is often the transition/migration phase from one IT system to the cloud

Cloud security concerns

- Evolving threat vectors
  - Increase in targeted cloud attacks as it becomes predominant
- Effective realization of the shared responsibility model
- Global optimization & standardization VS regional & nation-state priorities
- Compliance regimen
- Data protection, resilience, managing complexities
- Security at scale
- Cloud security workforce readiness

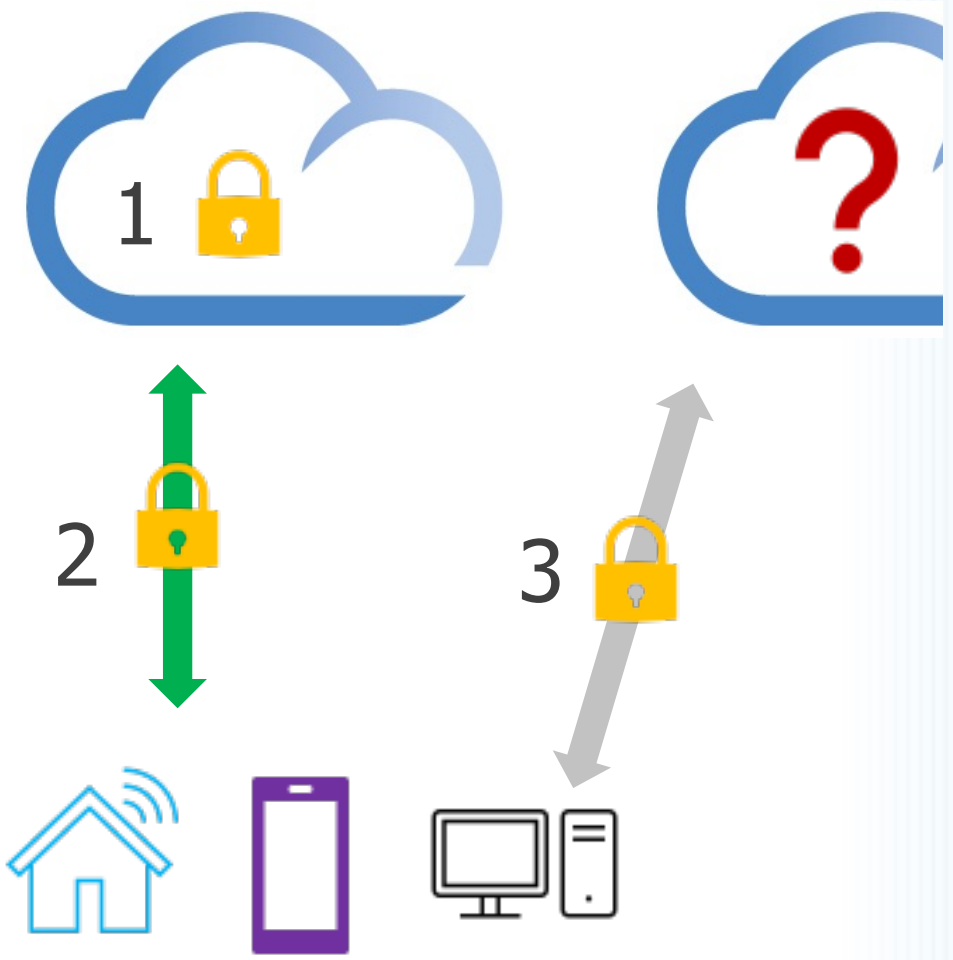
Top Threats to Cloud Computing

- Regular effort by CSA to quantify most serious and likely security issues to expect in the cloud
  - https://cloudsecurityalliance.org/group/top-threats
- "Bread and Butter" tenant security issues
  - Configuration, change control, patching
  - DevOps: poor API security, credential & key mgt failures
  - Lack of multifactor authentication & IdM strategy
  - Vendor due diligence & visibility
- Closer tracking of CSP vulnerabilities due to cloud criticality
- Cloud critical mass leading to targeting: e.g. cloud-specific ransomware



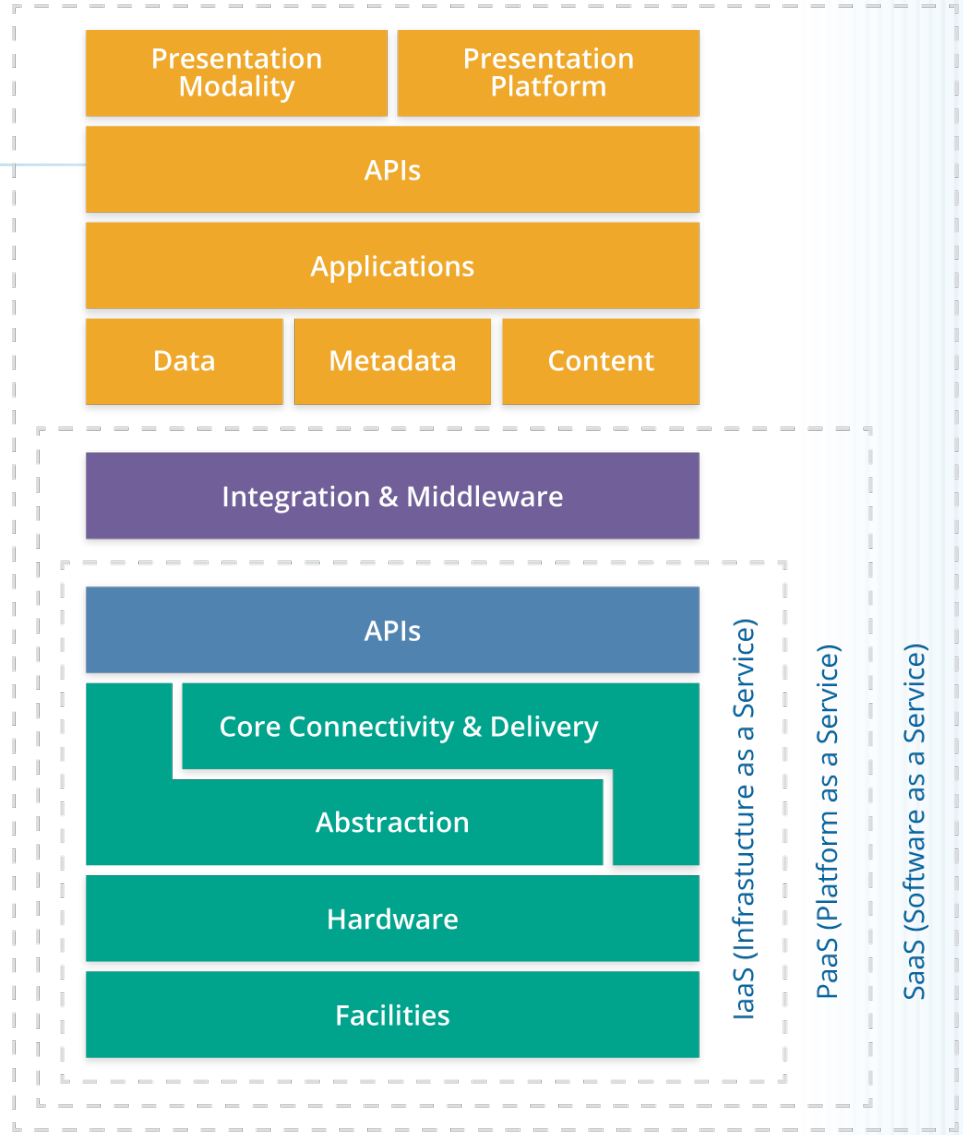
Cloud Definitions Frame Your Cybersecurity Strategy

1. Securing your Clouds	IaaS/PaaS/SaaS
2. Securing Edge to your Clouds	**Zero Trust**, Software Defined Perimeter/SASE
3. Edge/On premise to Third Party Clouds	Supply Chain



What Is Cloud Computing?

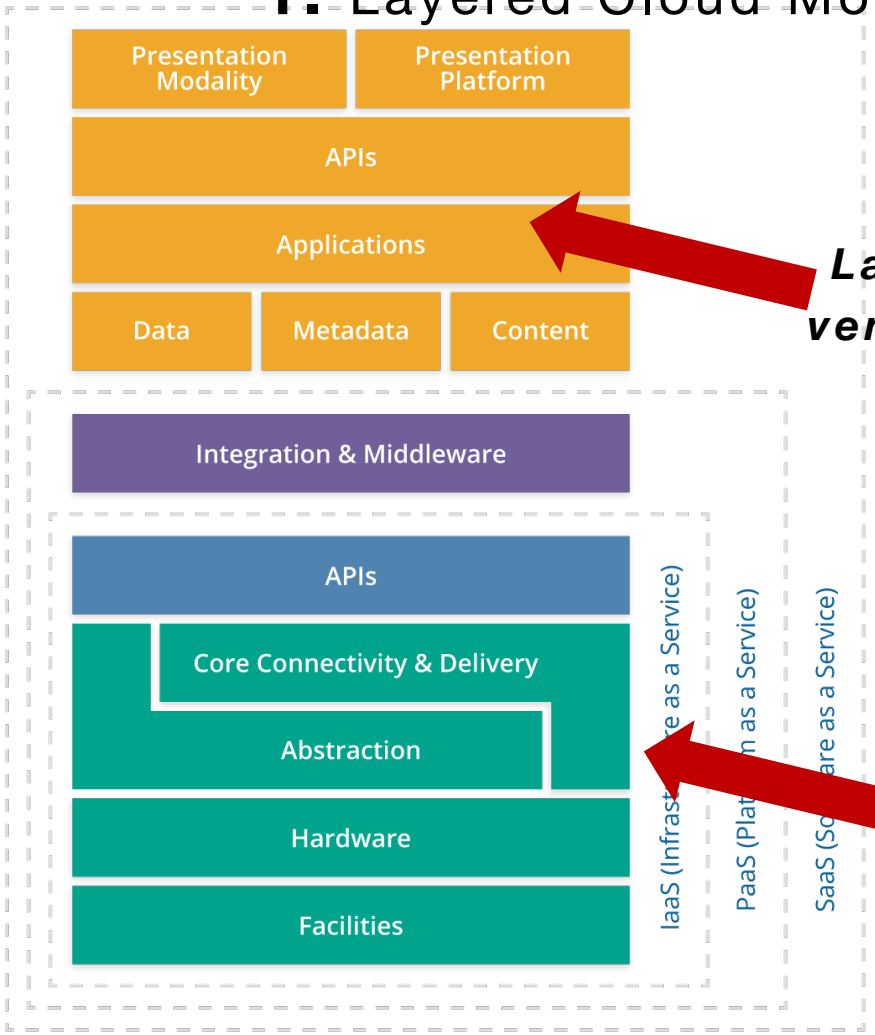
- On demand provisioning of compute as a service
- API-centric utilization
- NIST developed the most popular definition: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- CSA created a layered model to visualize SaaS/PaaS/IaaS



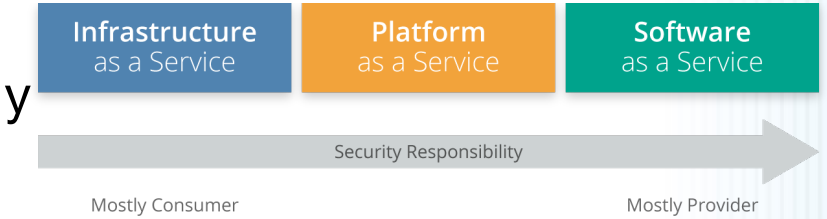
CSA Cloud Reference Model

Security Of The Cloud

1. Layered Cloud Model

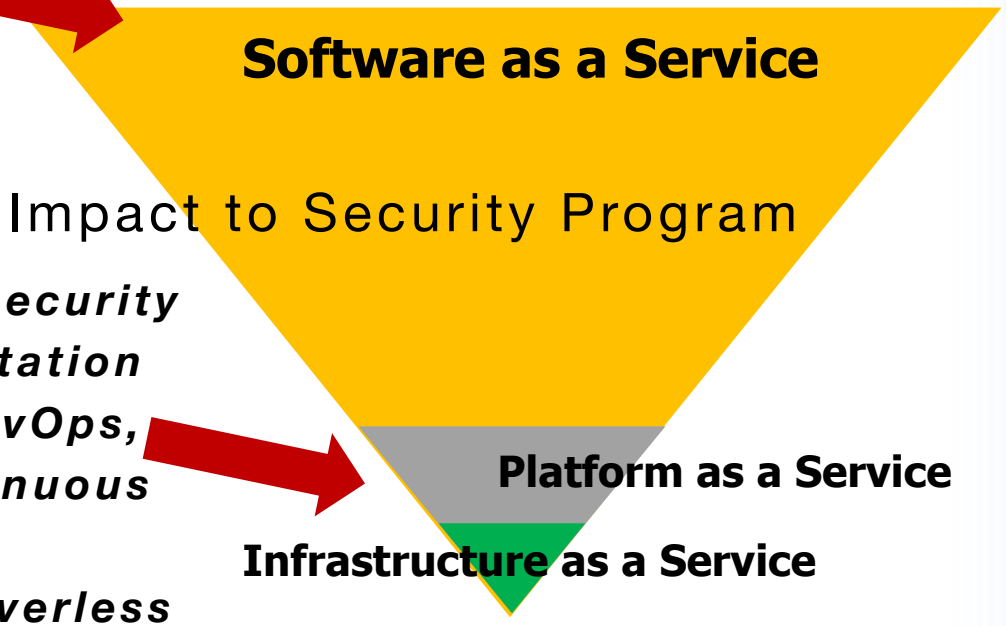


2. Shared Responsibility



Larger number of vendors for vetting

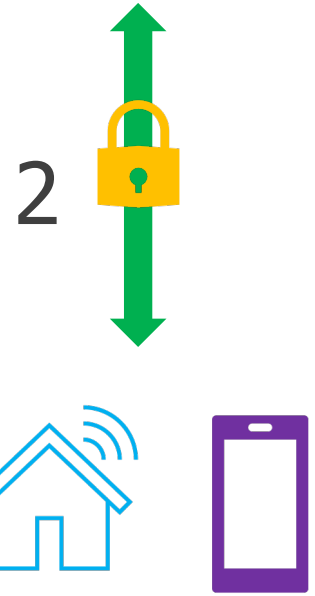
3. Impact to Security Program



Greater technical security control implementation responsibility: DevOps, DevSecOps, Continuous Deployment, Microservices, Serverless

Zero Trust: Securing Cloud To The Edge (And Edge To The Cloud)

- Zero Trust: strategy to implement least privilege
- Connecting corporate endpoints securely to corporate cloud assets
- Cloud managed edge devices such as Internet of Things, Autonomous Vehicles, Smart Cities, etc.
- Zero Trust, SDP, SASE, microsegmentation are major trends



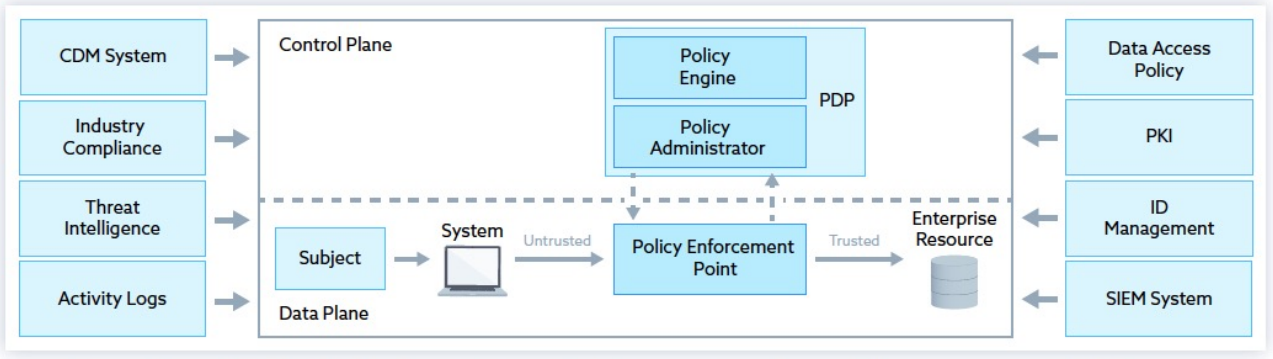
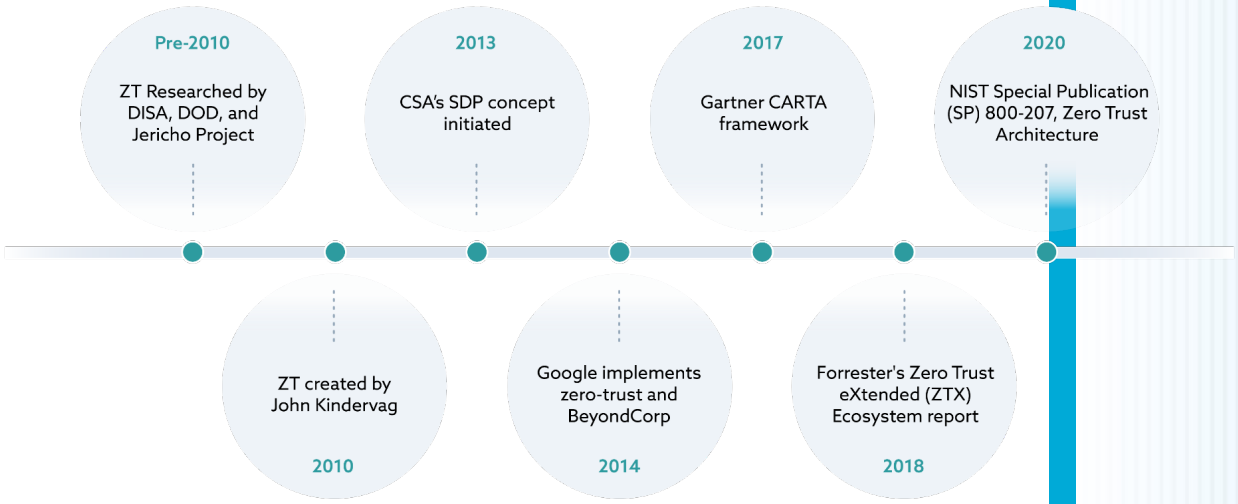


Figure 1: Source: NIST, 800-207, Zero Trust Architecture 2nd Draft https://csrc.nist.gov/publications/detail/sp/800-207/draft

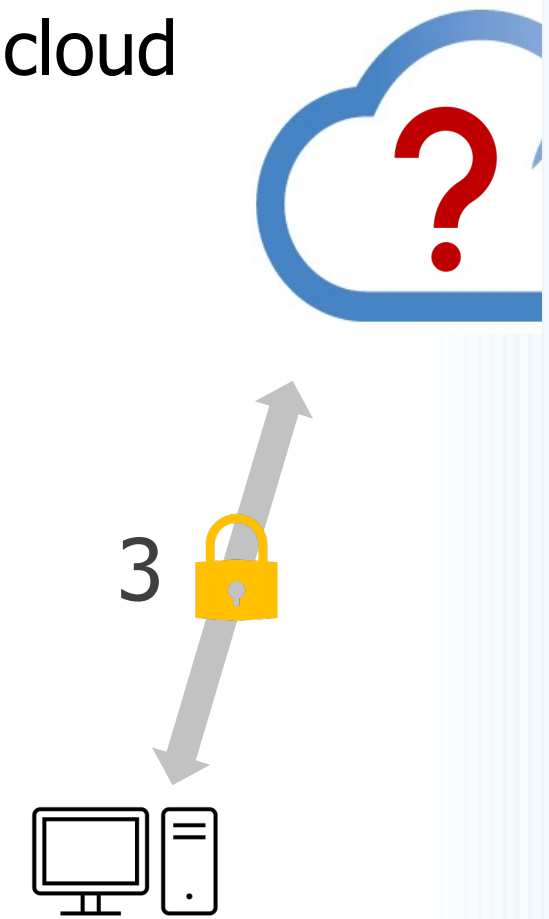
Zero Trust As Philosophy & Strategy

- Zero Trust: popular “re-emerging” strategy for protecting organizations’ digital personae
- Assumes all components are subject to compromise
- Emphasizes:
  - Protect assets with least privilege access
  - Identity as a foundation
  - Continuous verification
- Zero Trust aligns with the software-defined organization



Hidden & Persistent Cloud Connections

- Systems with connections to a command & control cloud host
  - Managing IoT firmware
  - Provisioning access
  - Updating systems software
  - Example: SolarWinds
- Cloud access hiding in plain sight
- Critical attack vector for sophisticated one-to-many attacks
- A major supply chain issue for 2021!



CISO views on the Cloud

- Apply risk mgt tools to **new threat vectors**
- IaaS adoption **“lowers the overall basket of risk”** compared to on-premise
- **SaaS is more problematic than IaaS** for security due to lack of organizational transparency – easy for business units to bypass IT/Security
- **Compliance more difficult** than technical cloud security due to audit/regulatory awareness
- **Dynamically updated technology stacks** drive need for **continuous auditing and assurance**
- **Serverless** computing and similar advances requires **rethinking** existing security controls
- **Adaptive** is continuous, automated & scaled cybersecurity on demand

Common Cloud Security "Functionality"

- Tools rapidly adding features, making it difficult to keep product categories
- "Cloud Native" versions of tradition security categories: SIEM, Log Mgt, Vulnerability Management, e.g. CSPM, CWPP
- Cloud Access Security Broker (CASB) & Secure Access Service Edge (SASE)
- Cloud Identity Management
- Cloud Workload Management & Orchestration: not exclusively about security, but critical to achieving security
- Cloud Security Posture Management
- Encryption & Key Management
- Data protection, e.g. solutions specific to storage buckets
- Security as a Service: secure the cloud, but also secure non-cloud assets, e.g. endpoints, Internet of Things
- Lots of innovation happening, don't assume last year's knowledge is current

Cloud Assurance Trends

- Standardized assessments
- Assessment sharing
- Lightweight
- Control inheritance
- Continuous / Automation
- Derivatives, e.g. security ratings

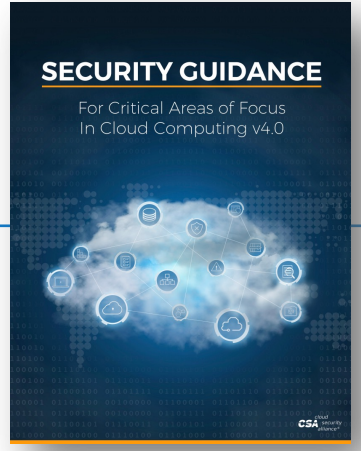
Just for Fun! Game changers

- “Snowden” Cloud
- Cloud Balkanization
- Privacy “Y2K”
- Human-less AI Cyber attack & defense
- Ransomware as Extortionware

Summary

- Cloud & Cybersecurity have an accelerated pace of change
- Cloud is dominating IT and Cloud Security is the foundation for Cybersecurity
- Reimagine Cybersecurity strategy via Cloud Definitions
- Build the Software-Defined Organization
- Zero Trust as a Philosophy & Strategy
- Security at Scale
- Cloud Native Security
- Level up Cybersecurity Skills

Popular CSA Research



CCAK
Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential

CCM
Cloud Controls Matrix

CCSK
Certificate of
Cloud Security Knowledge

CSA STAR

- Security Guidance
  - https://cloudsecurityalliance.org/guidance
- Top Threats
  - https://cloudsecurityalliance.org/group/top-threats
- Cloud Controls Matrix (CCM) & STAR registry
  - Popular security controls framework & CSP assessments
  - https://cloudsecurityalliance.org/group/cloud-controls-matrix/
  - https://cloudsecurityalliance.org/star
- DevSecOps
  - https://cloudsecurityalliance.org/research/working-groups/devsecops/
- Modern Cloud Architecture: Microservices, Serverless, SDP, Key Mgt
  - https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter-and-zero-trust/
  - https://cloudsecurityalliance.org/research/working-groups/containerization/
  - https://cloudsecurityalliance.org/research/working-groups/serverless/
  - https://cloudsecurityalliance.org/research/working-groups/cloud-key-management/

Thank You

Jim Reavis, Chief Executive Officer
Cloud Security Alliance
www.cloudsecurityalliance.org