Cloud Security: Key Considerations Across AWS, Azure & GCP

Brad Voris

www.VictimOfTechnology.com www.github.com/bvoris

Brad Voris, (a whole bunch of acronyms)

- Technical Security Manager @ Pharma Company
- 25 years of experience IT/IS/CS
- Undergrad in Cybersecurity @ Wilmington University
- Certifications: CISSP, CISM, CCSP, CCSK, Network+, MTA, MCP, etc.
- Co-Author 2 books: Intrusion Detection Guide and Essentials of Cybersecurity for Peerlyst
- Cloud Security Alliance Zero Trust Training Contributor
- **NOT AN EXPERT**

www.VictimOfTechnology.com www.github.com/bvoris

Why Cloud Security Matters

45% of data breaches involve cloud-based infrastructure

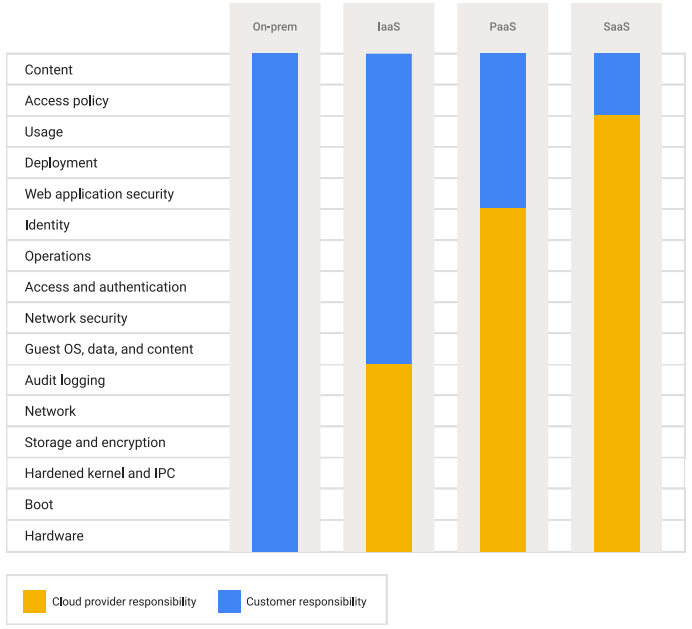
$4.35M average cost of a cloud breach (Source: https://www.ibm.com/reports/data-breach)

Oh and the Oracle Data Breach… that just went public…

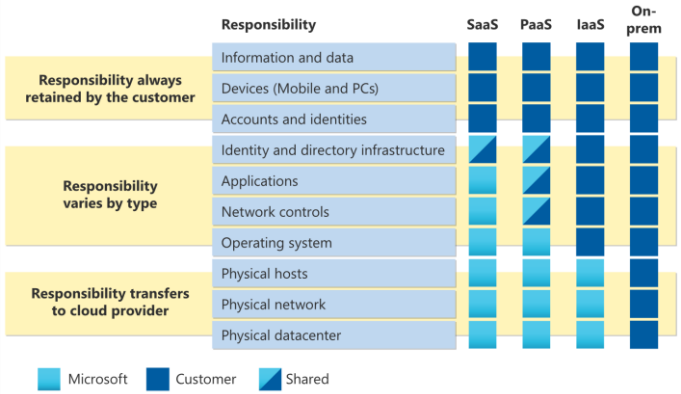
6M records exfiltrated from SSO and LDAP of Oracle Cloud (Source: https://www.cloudsek.com/blog*)**

Shared Responsibility Model

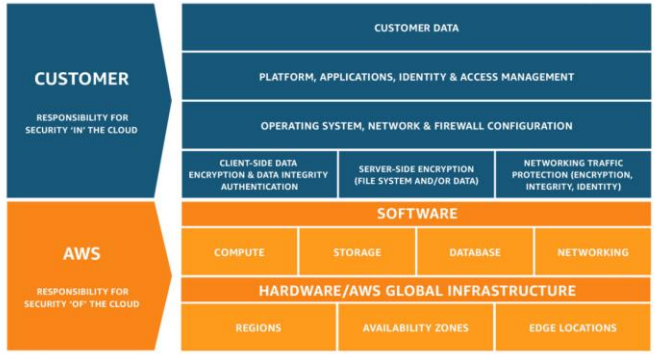
Google Cloud



Microsoft



aws



www.VictimOfTechnology.com www.github.com/bvoris

Identity and Access Management (IAM)

Key Considerations:

- Principle of Least Privilege (PoLP) / Zero Trust Architecture (ZTA)
- Multi-Factor Authentication (MFA)
- Role-based access control (RBAC)
- Attribute-based access controls (ABAC)
- Converged IDP vs. Non-Converged IDP

Architecture Components:

- AWS: IAM, AWS Organizations, Cognito
- Azure: Azure Active Directory (AAD) / Entra ID, Privileged Identity Management (PIM), Conditional Access
- GCP: Cloud Identity Platform, Cloud IAM

Data Protection

Key Considerations:

- Encryption at rest and in transit
- Tokenization and masking
- Backup and disaster recovery strategies
- Segmentation or data isolation

Architecture Components:

- AWS: KMS, Secrets Manager, S3 encryption
- Azure: Key Vault, Disk Encryption, SQL TDE
- GCP: Cloud KMS, Cloud DLP, Cloud Storage encryption

Network Security

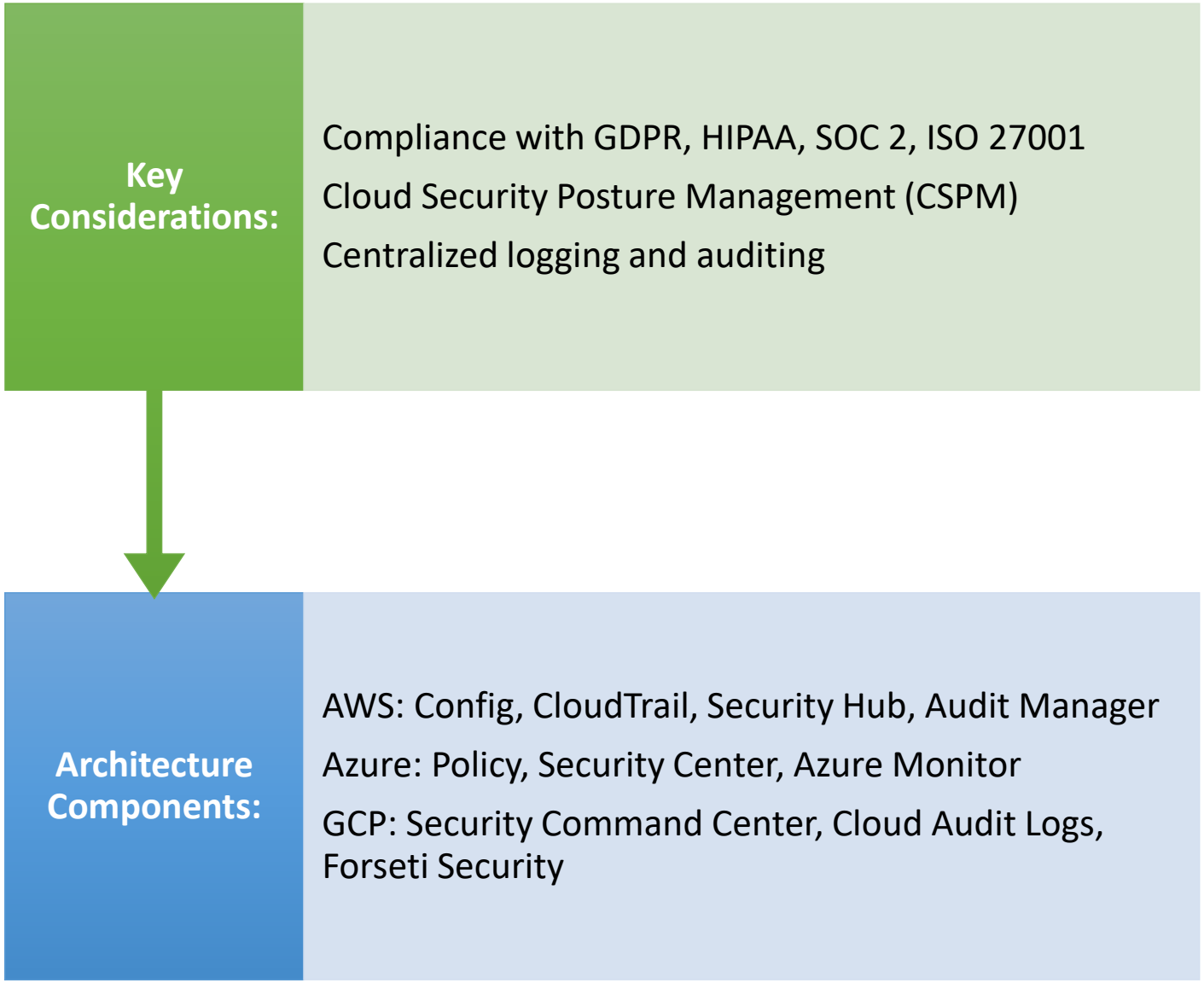
Key Considerations:

- Firewalls and Network Security Groups
- VPC/VNet segmentation / logging
- Web Application Firewalls / Proxies
- Zero Trust Architecture

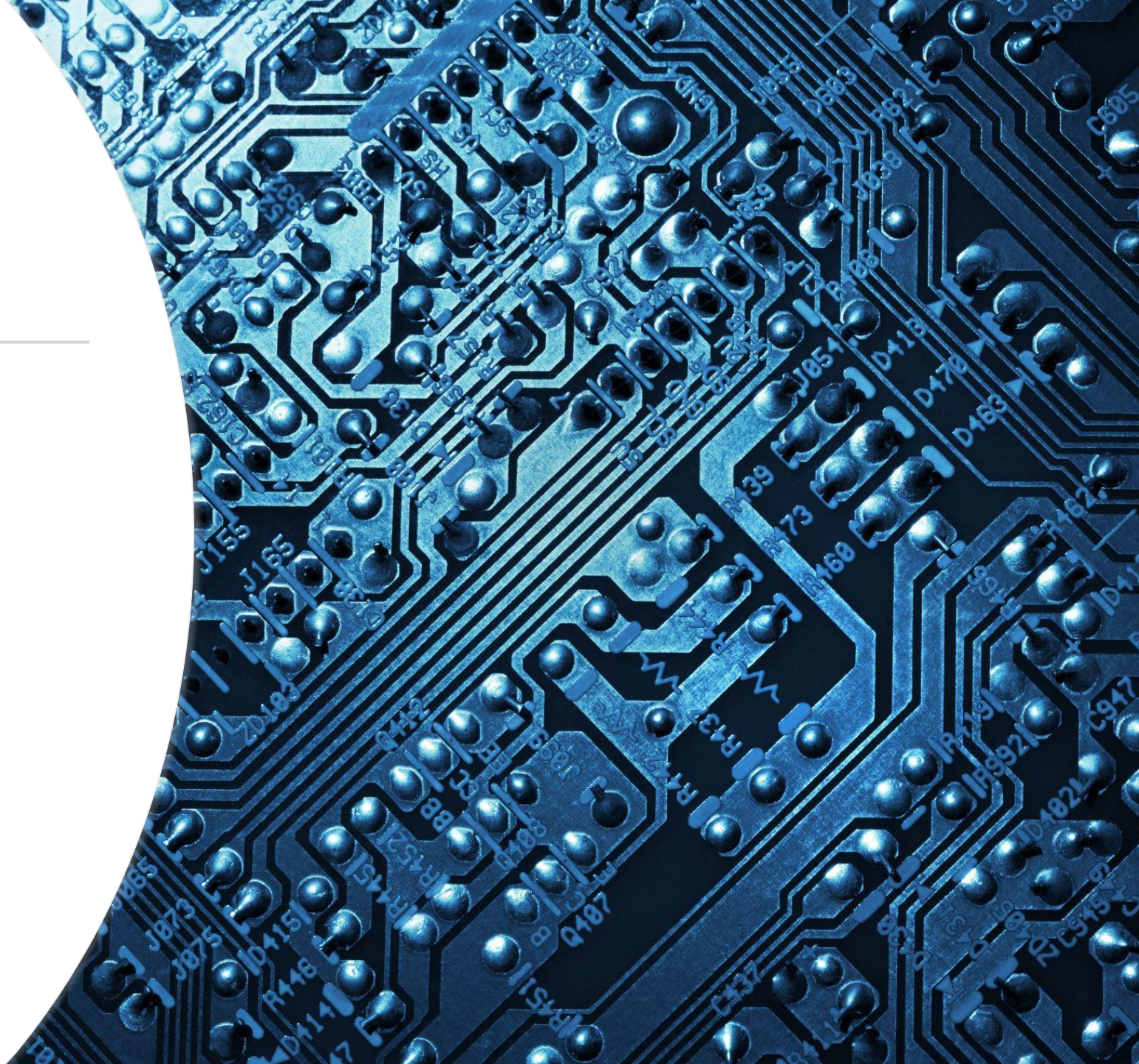
Architecture Components:

- AWS: VPC, Security Groups, NACLs, AWS Shield (DDoS protection)
- Azure: VNet, NSGs, Azure Firewall, DDoS Protection
- GCP: VPC, Cloud Armor, Cloud Firewall

Compliance and Governance



Threat Detection and Response



Key Considerations:

- Automated threat detection
- SIEM and SOAR integration
- Incident response automation

Architecture Components:

- AWS: GuardDuty, Detective, AWS WAF
- Azure: Sentinel, Defender for Cloud
- GCP: Chronicle SIEM, Security Command Center, Cloud IDS

Best Practices and Recommendations

Key Considerations:

- Adopt Multi-layered Security: Defense-in-depth approach
- Multi-cloud approach if possible
- Implement Zero Trust Architecture Methodology
- Automate Security: Infrastructure as Code (IaC)
- Regular Audits & Penetration Testing: Identify vulnerabilities
- Backup and Disaster Recovery: Ensure redundancy and failover strategies

Cloud Security is a Shared Responsibility

Q & A