Cloud Security by Default
The Rewards of Standards and Infrastructure as Code

George Holbert, Matthew Stout
University of California, Office of the President
ABOUT US

University of California
Office of the President
About Us

University of California:
• 10 Campuses - undergraduate/graduate
• 6 Academic Health Centers
• 3 National Laboratories
• >230,000 employees
• >280,000 students

University of California, Office of the President (UCOP):
• Systemwide infrastructure services
• Local infrastructure services
• >2000 employees
• >$2M annual cloud provider utility
• > 50 cloud accounts
### Our Cloud Journey

<table>
<thead>
<tr>
<th>Year</th>
<th>Cloud Exploration</th>
<th>Assessment</th>
<th>Foundations</th>
<th>Scaling</th>
<th>Even More</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 2019</td>
<td>Training for all</td>
<td>Established FinOps</td>
<td>Cloud Standards</td>
<td>Central IT Alignment</td>
<td>Containers</td>
</tr>
<tr>
<td></td>
<td>Freeform builds</td>
<td>Analyzed Existing Workloads</td>
<td>Automated Compliance</td>
<td>Retrofits</td>
<td>Cloudfront</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Easy Optimizations</td>
<td>Security Framework</td>
<td>Intermediate Optimizations</td>
<td>Cloud team and Infrastructure both supporting Cloud services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Migrations: UC Systemwide Payroll System</td>
<td>Migrations: Data Center (secondary)</td>
<td>Migrations: UC Systemwide Student Application System</td>
<td>Migrations: UC Systemwide Retirement and Pension Administration System</td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Starting to move one of DCs in full to Cloud in 2024</td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECURITY BY DEFAULT
Security By Default

• We now have ~50 accounts and more staff working in the Cloud

• The Cloud is now our default location for new services
  • More teams than ever with access to cloud accounts
  • More teams building resources
  • More potential for chaos and security incidents

• We also require consistency
  • We have centralized teams database administration, networking, middleware, infrastructure, security, cloud and fin ops that support all managed accounts
  • Even if security was not a concern we cannot be effective if we let every account owner choose their own standards
Security by Default

• With Security by Default we get
  • Consistency across accounts
  • Ability to audit or review risk faster per account or service
  • Most baseline standards met before anything is built
  • Builds are faster once we have a standard and reuse lessons learned or we have standard solutions
  • New solutions and services deal with Security standards or controls from the beginning not later just before going live
Security by Default

• Today we will look at three of the main ways we implement our Security by Default

• However, first let's look at the complexity of Security and just how much we are trying build into our cloud offerings
SECURITY AND STANDARDS

They can be their own chaos, even while saving you from far worse chaos
Our Tool Box

- AWS Trusted Advisor
- AWS Organizations
- Amazon Inspector
- AWS Security Hub
- AWS Well-Architected Tool
- Amazon GuardDuty
- AWS IAM Identity Center
Our Tool Box

• That previous slide is not an attempt to dazzle, nor confess that we might have too many tools, rather we want to make a case for how difficult all this would be without our standardization and security setup in all accounts.

• Next, we will look at just a few of those tools and how they are useful to us, but also how complex they can be.
Security Hub

- AWS Security Hub is a cloud security posture management (CSPM)
- AWS maintains standards with hundreds of checks
- Helps prioritize the most sensitive issues
- Gives your overall status
- ~250 checks (just the ones we have in use!)
Trusted Advisor

- Checks to aid in following AWS best practices
- ~200 checks
- Enterprise Support customers: AWS Trusted Advisor Priority
- Does require support to get all checks
GuardDuty

- Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
- We see variable findings but it can be dozens a month across accounts at times.
Cloud Custodian

- Flexible, simple configuration syntax to find resources and apply actions.
- Unlike other tools you can easily take actions on a resource
  - Such as set IMDS v2 on in all accounts
- We have ~30 policies to set encryption on if not, automate S3 access logging, and much much more

https://cloudcustodian.io/
Security and Operations Tools

• In addition to those there are more than we can cover in this talk
• They included
  • Host vulnerability management solution
  • Web application Scanning
  • Endpoint Detection and Response EDR
  • Security Information and Event Management SIEM
  • Central authentication and access logging and alerting
  • Central Performance Monitoring Solution
  • CloudWatch
  • And more
Summary By the Numbers

• Security By Default Means from the start we want to meet all of these:
  • Security Hub: ~250 checks
  • Trusted Advisor: ~200 checks
  • Cloud Custodian: ~30 policies active

• Over 500 Checks not including vulnerability scanning, automation to install agents for scanning, etc.

• Up Next: Three ways we handle Security by Default
  • AWS Account Setup
  • Infrastructure as Code (IaC)
1) Governance
Account Creation and Setup

• A must for
  • managing so many accounts
  • shared teams and
  • adopting standards...

• As important as any software or technical solution
  • See that timeline at the beginning of this slide
  • Our cloud journey had many important steps of setting up standards, roles and responsibilities and building our different teams we never had before
2) Account Setup

Start with Security All In
Account Creation and Setup

• We use AWS Organizations
  • Our automation is a bit lacking; several separate processes and a few manual items, however, is very similar to Control Tower
    • Separate network, logging, security accounts
    • AWS SSO, SCPs, etc.

• We start from day one in all new managed accounts with all of standard controls and setup
  • Security Hub, AWS GuardDuty, Enterprise Support, and all the rest
  • We rarely do POC accounts and if we do we still do all the same setup
  • Rarely allow unmanaged accounts, mostly legacy or special use
  • This means as new services are created or resources deployed we catch configuration or security issues at the start
Infrastructure as Code (IaC)

How we build in AWS
What Is Infrastructure as Code (IaC)?

• Infrastructure as Code (IaC) is the managing and provisioning of infrastructure through code instead of through manual processes.
• Examples include:
  • AWS CloudFormation, Red Hat Ansible, Chef, Puppet, SaltStack and Terraform.

• With IaC we can build:
  • VPCs in a few minutes
  • Same for EC2, Load Balancers, ECS+Fargate, and much more
  • This allows a few experts to build faster when they are the ones that must
  • We are working to make more of our standard builds things all on the Cloud and Infrastructure teams can build
What We Use

• Terraform
  • Terraform is our primary tool of choice for all our AWS Cloud resources
  • Terraform codifies cloud APIs into declarative configuration files
  • Great public examples, modules, and code
    • [https://registry.terraform.io/](https://registry.terraform.io/)

• Use Modules
  • Modules have the main code and do all the creations and we only need a small block of code to supply the variables and options we want on a resource
  • See our slides from last year for more!
What We Use

• IaC is not just terraform or similar solutions!

• Other Examples – Other ways we to add IaC:
  • Automated container deployments via CodePipelines/commits to version control
    • Allows app developers to write code and deploy it
  • Systems manager Documents
    • Automate security agent installs, join domain, and more. Mostly windows for us now
  • Puppet for Linux
    • Harden OS, install security agents, and more
CONCLUSION
Security By Default

- Reduce the time involved in reworking or redesigning solutions
- Create in an environment with all of our standards and enforcement tools
  - Sometimes slows us down at the start, however, this resolves issues early and not while rushing to release production

- Security we can mostly forget and still have in place
  - Allow more hands to start building while still keeping us secure
  - Security by Default!
Questions?
UCOP @ Technology Exchange

• Join us for our 2023 Technology Exchange presentations by UCOP team members:
  • **Moving from VM to Cloud Native Containers** with Khalid Ahmadzai, Tuesday 11:20am-12:10pm
  • **Cloud Security By Default** with Matthew Stout and George Holbert, Thursday 10:20am-11:10am
  • **Control Chaos with IaC & Automation** with Josh Whitlock, Thursday 1:40pm-2:30pm
  • 2022 Technology Exchange presentation by UCOP’s own Khalid Ahmadzai, Kari Robertson, Matt Stout
  • **Moving from Cloud Chaos to Standards:**
QUESTIONS