DON'T JUST LIFT AND SHIFT!

WHY TRADITIONAL CONTROLS DON'T ALWAYS APPLY TO THE CLOUD AND WHAT YOU CAN DO ABOUT IT

WHO AM I

Steve Turner

Director, Security Architecture @ Prudential

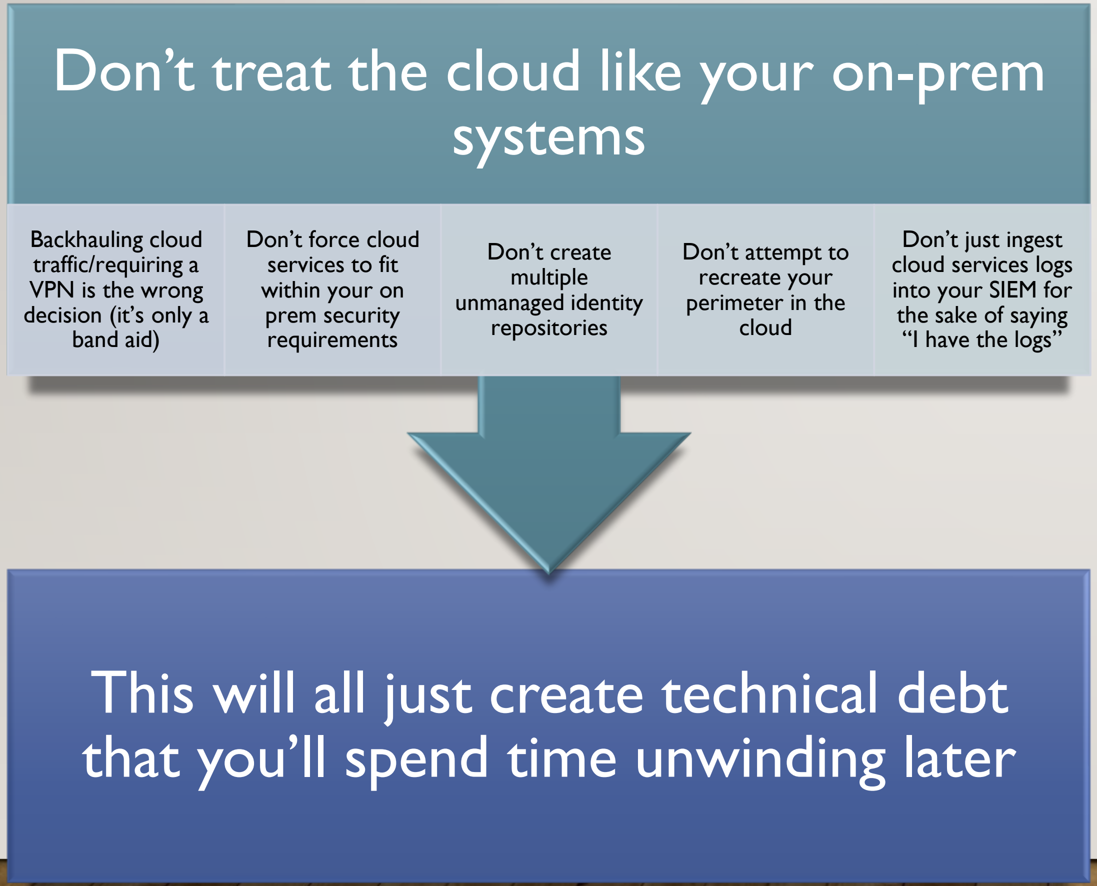
Twitter: @beingageek

LinkedIn: linkedin.com/in/beingageek/

IT Infrastructure – 6 years

Infosec – 6 years

CLOUD JOURNEY MISTAKES!



Don’t treat the cloud like your on-prem systems

Backhauling cloud traffic/requiring a VPN is the wrong decision (it’s only a band aid)

Don’t force cloud services to fit within your on prem security requirements

Don’t create multiple unmanaged identity repositories

Don’t attempt to recreate your perimeter in the cloud

Don’t just ingest cloud services logs into your SIEM for the sake of saying “I have the logs”

This will all just create technical debt that you’ll spend time unwinding later

CLOUD JOURNEY LESSONS LEARNED

Look at cloud provider native controls to centralize your security visibility and controls where possible.

Invest in a centralized identity strategy (provisioning/deprovisioning/authentication) and determine your source of record

Reevaluate your network needs and implement solutions that don’t require you to backhaul all your network traffic with something such as a Secure Web Gateway

Implement a Cloud Access Security Broker (CASB) to help centralize monitoring/ remediation/governance across Cloud Services

Reevaluate your log and monitoring strategies along with the capabilities of your SIEM

Automation and Orchestration are your best friends

Shift your processes and people to leverage or upskill areas where you're lacking

CORE RECOMMENDATIONS ACROSS CLOUD SERVICES

Review Security Roadmaps if Available, Look for Security Recommendation Guide/Whitepapers

- Look at NIST, CIS, and other benchmarks

Setup SSO/Federated Identities to all cloud services with MFA enabled

- Monitor unfederated accounts
- Monitor and restrict authentication token lifetimes
- Become familiar with process around terminating/invalidating access tokens

Secure Root/Administrative Credentials (enable MFA, enable alerting when used, etc.)

- Monitor and rotate access keys for applications and service accounts

Ingest and alert off relevant logs into your SIEM

CORE RECOMMENDATIONS CONT'D

Connect all your cloud services to a CASB/SWG for centralized visibility and controls

- The level of integration will vary between cloud providers, but selecting the right solution should allow you some level control across ALL cloud providers
- Allows insight into Application Integrations for your SaaS apps
- Establish central policies across cloud providers that will alert you to general badness
  - Anomalous Detections (baselining normal activity and alerting off abnormal behaviors)

Enable Data Encryption

- Most cloud providers have native encryption available, turn it on!
- If not natively available, some CASB's are able to do this

Set Password Policies even if you're federated

- This forces unfederated accounts to have a similar, if not the same, password policy as your org

NATIVE CONTROLS

- Lucky for us, the big cloud infrastructure players have in recent times made a lot of assessment/detection/remediation easy
- Central Hubs for all security data
- A way to get it out to SIEM for additional analysis
- Security telemetry and controls all throughout their ecosystems
- SaaS providers are getting better at offering controls, telemetry, and overall auditing

  There are some premium plays as well

  - Examples: Salesforce Shield, Microsoft 365 E3 vs E5, etc

ADD ON CONTROLS

For all the other SaaS cloud providers, we've got options! (or if you're just sick and tired of death by a thousand cuts for cloud DLC)

Cloud Access Security Brokers/Secure Web Gateways

- Provide a level of granular control and monitoring that's not normally available for SaaS apps
- Very easy to implement!
- Give significant benefits beyond security
- Most CASB's allow some level of control for ANY application

AMAZON WEB SERVICES (AWS)

- Recommendations
  - Turn on CloudTrail and centralize all logs to an S3 bucket that you ingest into your SIEM
    - Make sure that the logs can't be deleted, and they're encrypted
  - Utilize IAM Access Analyzer
    - Seriously, this will save your butt later, it lets you continuously evaluate your IAM roles to understand if someone accidently opened something they shouldn't have
  - Turn on Detective, GuardDuty, Inspector, and Macie and make sure that you turn on Security Hub
    - Security Hub will analyze all the data from the different security services and provide recommendations
      - ACTION these recommendations
      - Once you're comfortable, you'll want to automate those actions
    - Ingest and analyze alerts either in Security Hub or your SIEM
  - More resources and information below:
    - https://aws.amazon.com/blogs/security/top-10-security-items-to-improve-in-your-aws-account/
    - https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp-controls.html
    - https://github.com/aws-samples/aws-security-hub-response-and-remediation

MICROSOFT AZURE

- Recommendations
  - Turn on the Azure Security Center Standard licensing for all Azure Subscriptions
    - Seriously, this will give you an insane amount of useful, actionable data
    - Can do preventative controls as well
  - Enable Privileged Identity Management and MFA with Just-in-Time access to resources and administrative roles
    - This applies to Administrative Roles AND access to various Azure resources (VM's, microservices, etc)
    - Enables least privilege quickly
  - Centralize your logs into an event hub and setup a process to ingest into your SIEM or a Log Analytics workspace
    - This does require that you turn on the appropriate configuration in the various Azure services/tiers
      - https://docs.microsoft.com/en-us/azure/azure-monitor/platform/stream-monitoring-data-event-hubs

MICROSOFT 365

- Turn on Audit Logging!!!!
  - Natively, you can look at 90 days worth of logs
  - Ingest into your SIEM for additional analysis
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-troubleshooting-scenarios
- Change settings from the defaults: Anti-phishing, Anti-malware, Anti-spam
- Turn OFF Azure AD User Consent for Applications
- Turn on Conditional Access and MFA for your users and admins
  - Don't lockout your Global Admins!
- Turn on Identity Protection and Password Hash Sync (if federated)
  - Let's you take advantage of smart lockouts, IP lockouts, and discovering if you have leaked credentials
- Turn on Cloud App Security and at bare minimum the default threat protection and anomalous behavior policies
  - Ingest the alerts back to your SIEM!
- Pay to play in Microsoft 365 land
  - A lot of the key security benefits are baked into the Microsoft 365 E5 or other premium licensing
  - Awesome diagram here (It's all clickable): https://github.com/AaronDinnage/Licensing/blob/master/Microsoft%20365%20Enterprise%20on%20a%20Page.pdf
- Pay attention to Secure Score recommendations, dynamically change
- And so much more! https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-roadmap?view=o365-worldwide

SALESFORCE

- Turn on the appropriate auditing and monitor for anomalous behaviors
- Use the health check or org monitor if you have multiple tenants
  - Understand if you're utilizing Salesforce Security Baselines or if you're out of baseline
- Utilize Enhanced Transaction Security Policy
  - Allows for blocking and alerting on various Salesforce events
- Utilize some level of platform encryption that supports the native searches, workflows, and validation rules
  - Salesforce Shield is a good component to accomplish this
  - A lot of CASBs also support this, but your mileage may vary
- And So Much More! https://resources.docs.salesforce.com/224/latest/en-us/sfdc/pdf/salesforce_security_impl_guide.pdf

WORKDAY

- Get involved in high level security design, usually sits with your HR technology team
- Highly recommend integrating with a CASB
- Workday doesn’t have native analysis of anomalous events
- CASB can pull back ALL administrative and user activity including commands that are being run on Workday backend
- Useful for comparing and correlating against other applications within your org

MITRE ATT&CK® MATRIX CLOUD

- Updated to include cloud in October 2019.
- Fantastic starting point to understand where your org stands from a high-level
- Hasn’t been updated since then, so your mileage may vary
- https://attack.mitre.org/matrices/enterprise/cloud/

Q&A