
CIO VISIONS SUMMIT
Cybersecurity | Mid-Market | Leadership
Endre Jarraux Walls
Customers Bancorp
5 STAR REVIEWS
QUARTZ events.com

Cloud ‘Nine’

Architecting The Secure Cloud for Regulated Industry

About Me

- CISO for Customers Bancorp
- Regulated Industries: Banking, Healthcare, Food Manufacturing, Hospitality
- Serial Innovator
- Father of 4
- Philadelphia Eagles Fan since 1981

Don’t Be CHEAP…

- Cloud will cost less than a traditional datacenter, but only in hard costs.
- Proper planning will balance cost with security & scalability.
- Architecture selection and provider selection up-front are key to survival.
- Each provider brings their own advantages/disadvantages (Azure, Amazon AWS, Google Cloud)
- Containerization is the future but has challenges.
- Hire (or train) a cloud architect. Re-train your networking team to learn software-defined networking.

2

Start from Scratch

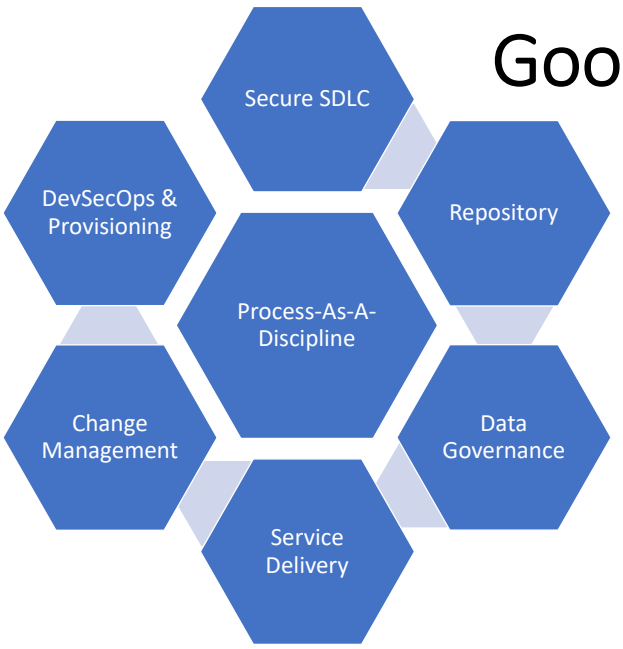
- Forget how you do it today. You might bring yesterday's crud with you.
- Architect your environment like new
- Keep a living master – Cloud environments do not present like traditional infrastructure. You'll need good "maps" to help you navigate the architecture and troubleshoot issues.
- Build for tomorrow NOT for present state.
- Design security as part of the architecture process – NOT as an add-on.

3

Process is Key

- Develop standards of operating procedure BEFORE you go to production.
- This includes critical tenets like Change Control

Good Process Hygiene



Good process hygiene will save you from cost overruns and security nightmares.

- Your secure SDLC processes should be well-aligned to your regulatory requirements and risk appetites.
- Repository is everything in cloud. Design it well. Secure it. Monitor it. And ensure it's kept away from production.
- Data sprawls quickly in Cloud. Design data flows up-front, identify storage points, decrease places where PII can live. Confine risk BEFORE data gets there.
- Service delivery is the key to everything. Even if your cloud won't serve the public, ensuring a process for delivery of service – incident response and handling, disaster recovery and prevention, patching & bug fixes, etc. is crucial to delivering a secure cloud that is immediately able to provide value to the org.
- Change Management – in a regulated industry you live and die by this discipline. Change management requires careful orchestration and demands consistent and careful documentation. If your process isn't good today, fix it, BEFORE you venture into the cloud. If you're already there, get good fast.
- DevSecOps = the intersection of DevOps and continuous security. If DevOps is good, DevSecOps is how you get to great. Security-aware implementers should have run-books for their operation, document everything, and implement solutions within the security perimeter the first time, everytime.

4

Know Your Tools…

- Some cloud providers offer deeper toolsets than others, but knowing what's offered is critical to ensuring a secure cloud.
- Make sure today's toolset in your Ops & Security departments are compatible with cloud (SIEM can ingest, Ticketing system, etc.)
- Perimeter security becomes more difficult – so do not expect traditional security here.
- Get creative with the right mix of provided and acquired tools to get the job done. Single pane of glass is both hard-to-find and unproven.
- Make sure your crew is trained. Make sure your security team aligns controls to the TOUGHEST standard to fit your org's risk tolerance.

5

1 Way In… 1 Way Out…

This is the hardest principle for executives to understand.

- In a traditional datacenter we have this by default. In the cloud you do not. Every machine provisioned has internet access BY DEFAULT
- Routing has to be controlled to point to a choke within the cloud perimeter.
- Security should be established to create predictable outbound traffic with well-known and expected inbound flows.
- Different clouds apply this principle different ways. But choking traffic is a principle to live by.

6

Know Your Role…

We use RBAC everyday. Cloud is NO different.

- An issue with cloud is that granularity is present – not the default.
- Discipline in implementing Role based controls is key to preventing people from having too much access.
- Development of a strong RBAC implementation in the cloud is absolutely critical. Be stingy, strategically.

7

Separate Dev From Prod

This is where it can “feel” expensive.

- A few options: Leverage traditional remnants for on-prem development and QA activities, or implement a separate cloud subscription for development and QA with linkages to the production environment for deployment, and tight controls around deployment capabilities.
- Encryption: Should be at-rest (actually encrypt your databases – the tenant is supposed to manage their own encryption), in-line (from server-to-server using private key pairs), and in-transit (from client to service/app).
- Logging locations should be encrypted as well. Logging facilities should be guarded at the same level as persistent data…logs give too much information so protect them well; and include that protection in the design.

8

Deploy Your Cloud Blue/Green

The idea of Blue/Green is running identical production environments to reduce downtime and improve availability. Updates are pushed to the blue environment while green continues to function. Then Blue is promoted to Green. Green is then updated and becomes Blue.

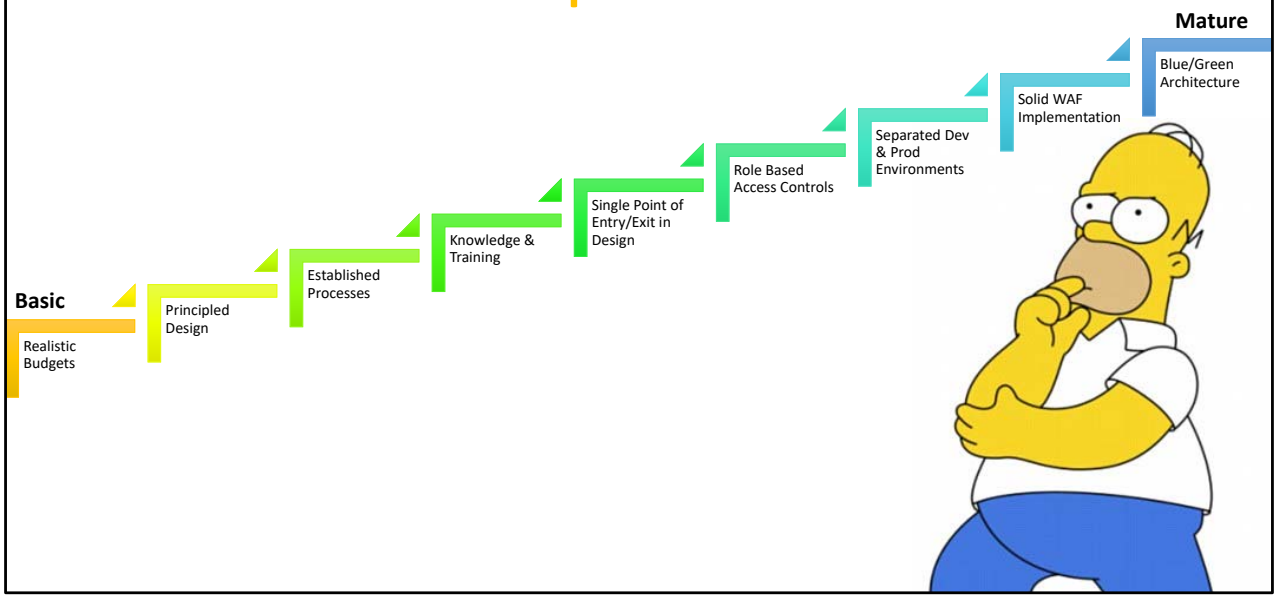
- If you operate in a 24x7x365 reality this is where cloud can save you lots of money, time, and resources.
- Geographic disbursement also becomes an option here.
- Your risk surface is actually changed by having the ability to balance across environments, making it tougher to target the entire infrastructure.

9

Get a Solid WAF!

- Web Application Firewalls used to be a luxury in traditional environments. In cloud environments they're essential. Your cloud identity is now a domain name, not necessarily an IP address…so leveraging a solid WAF to protect the ingress perimeter is absolutely key to deploying a secure cloud.
- Integrating the WAF with your security tools and obfuscating the real IPs of your systems through layered DMZs should be considered a best practice.
- DNS protection is also important. Use diverse DNS servers with DNSSEC and DKIM/SPIF on mail services.
- What makes a solid WAF is its ability to integrate with your cloud provider's application service architecture as well as DDoS protection and deep inspection with geo-IP controls. Other features like SSL proxy can provide new layers of protection not available with firewalls alone.

A Different Viewpoint…



Let's look at this a different way – if we apply these principles to a maturity scale, base maturity is forming realistic budgets, while achieving a blue/green architecture would make you significantly more mature than the majority of businesses who have ventured into the cloud space.

Stay Vigilant!

ewalls@customersbank.com
https://linkedin.com/In/endrewalls