

Mitigate Risks Using Cloud-Native Infrastructure Security

Agenda

- **Examine on-premises infrastructure security**
 - Are there any issues we want to avoid?
- **Examine cloud-native infrastructure security services**
 - Can these help address existing issues?
- **Let's build!**

Before we begin

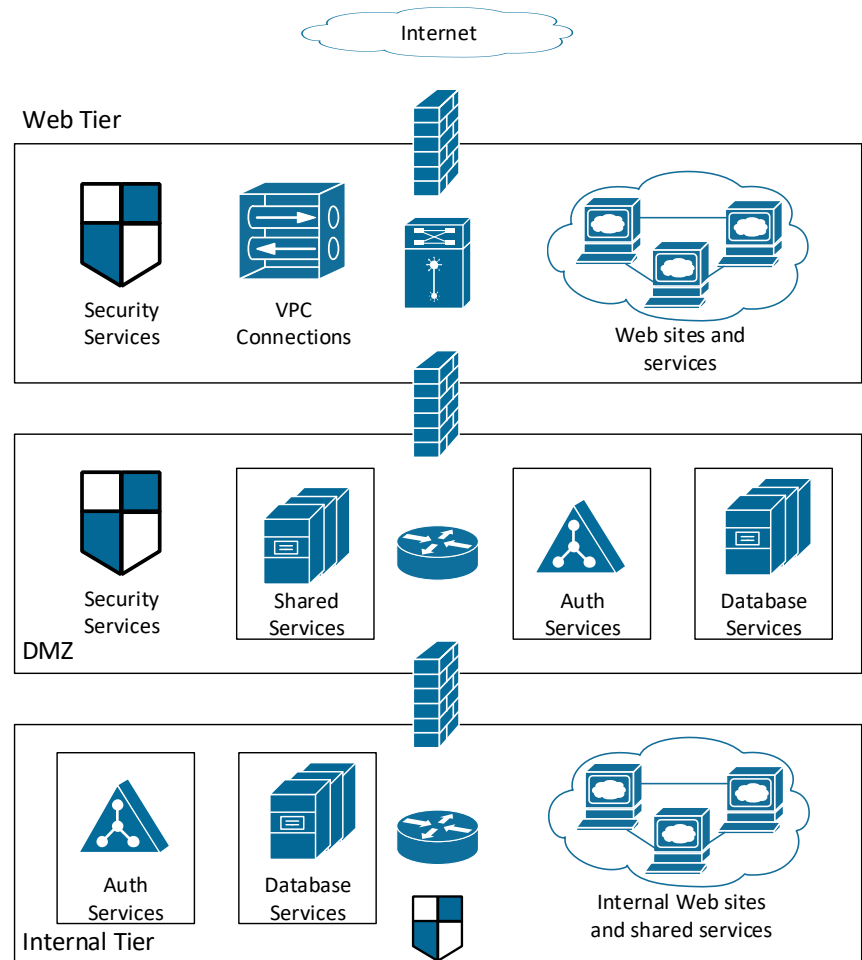
Start this session with a fundamental premise

When you're tempted to ask "Where is?", instead ask
"Why did I need?"

On-premises architectures

Network centric security

- Firewalls
- Multiple layers of network-based security services
- Routing & subnet Isolation

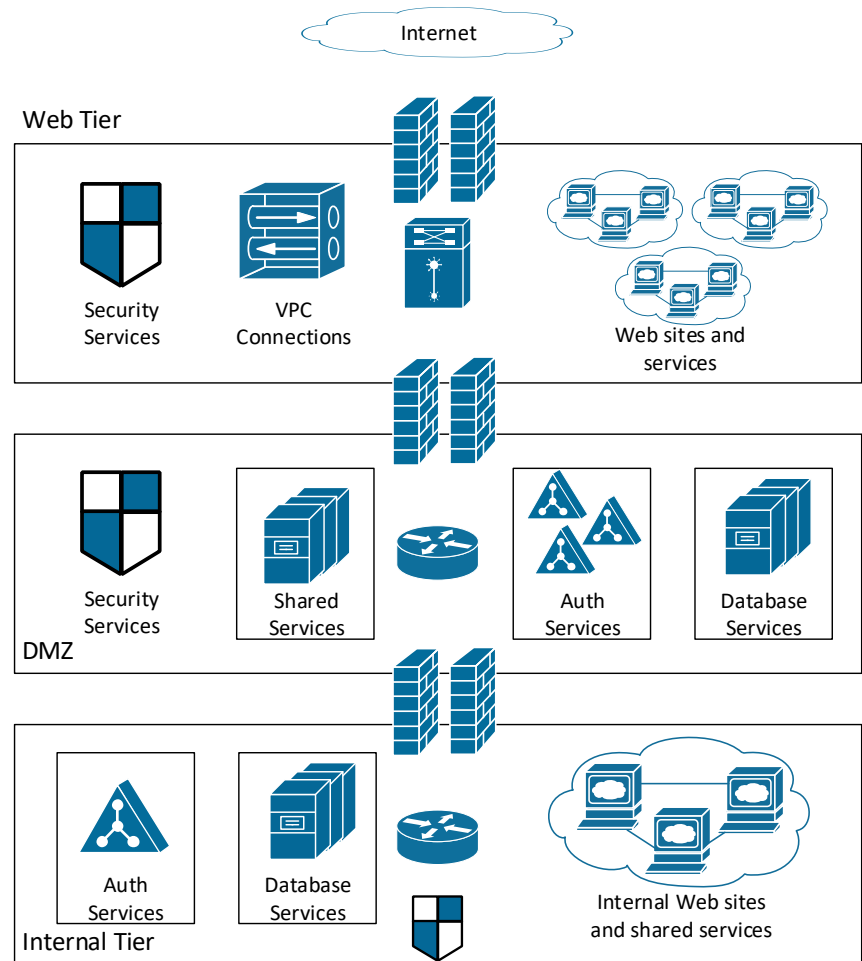


Reality is a little more complicated

Multiples of everything

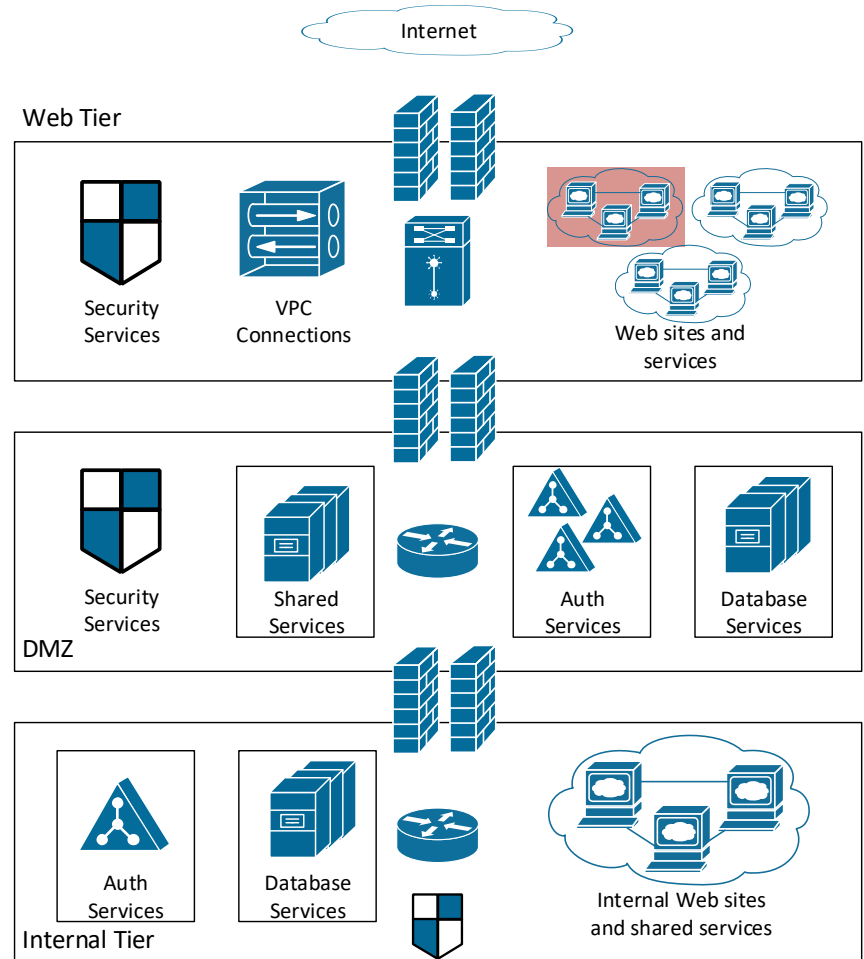
- Multiple firewalls
- Multiple services
- Multiple shared dependencies

What does this mean for isolation?



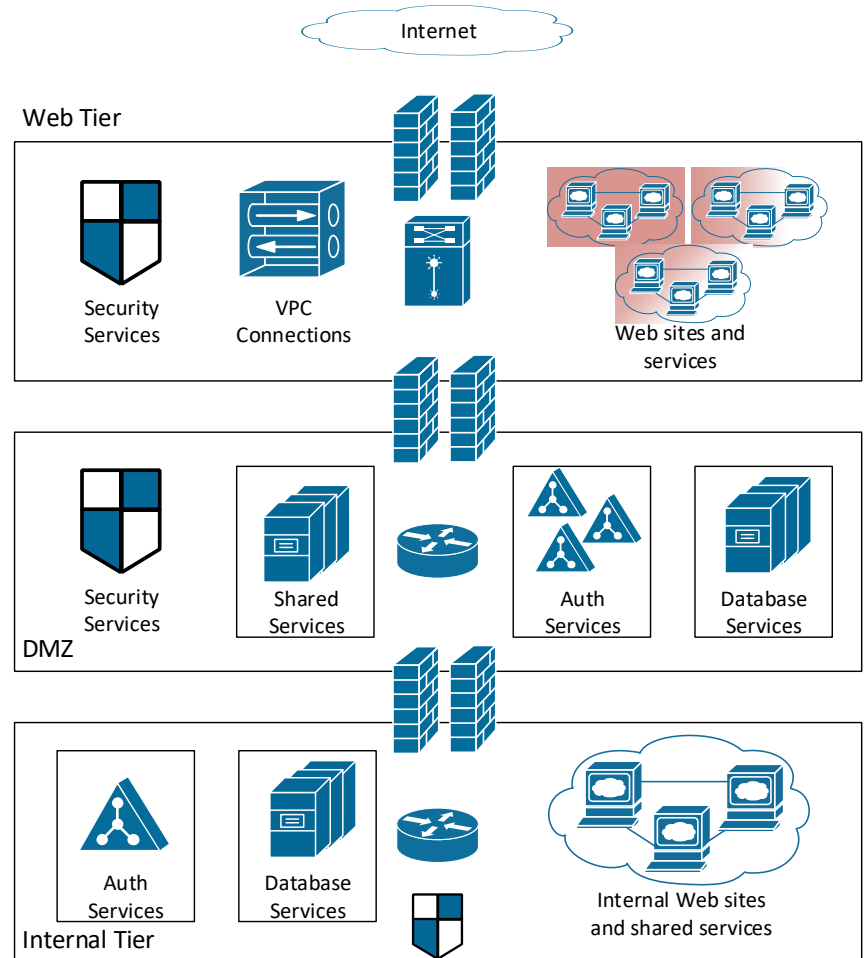
When an intrusion happens

What happens when isolation breaks down?



When an intrusion happens

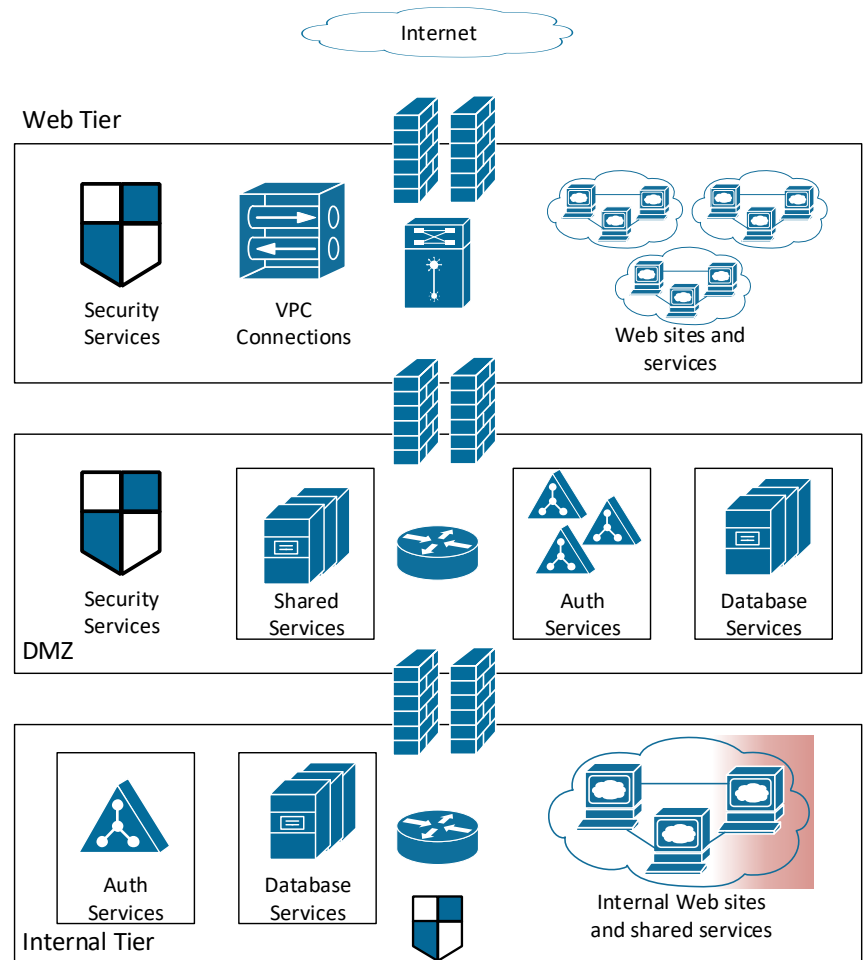
What happens when isolation breaks down?



When an intrusion happens

What happens when isolation breaks down?

What about your internal architecture? Change Management?

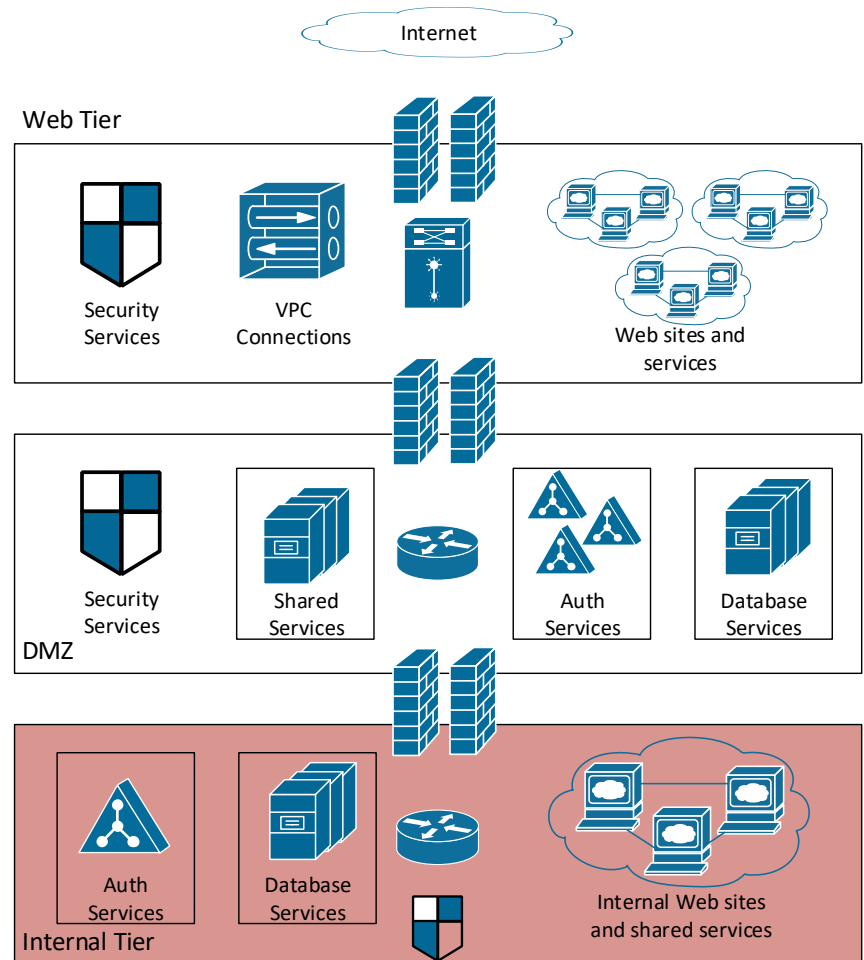


When an intrusion happens

What happens when isolation breaks down?

What about your internal architecture? Change Management?

Why would we want to copy this?



Reducing risks using cloud-native solutions

- Provide granular control
- Improve application isolation
- Lower operational burden
- Security insight across all environments
- Improved admin access
- Security Groups & NACL's
- Virtual Private Clouds
- AWS CloudFormation
- Amazon GuardDuty, AWS CloudTrail, AWS Config
- AWS Systems Manager

Cloud-native architectures

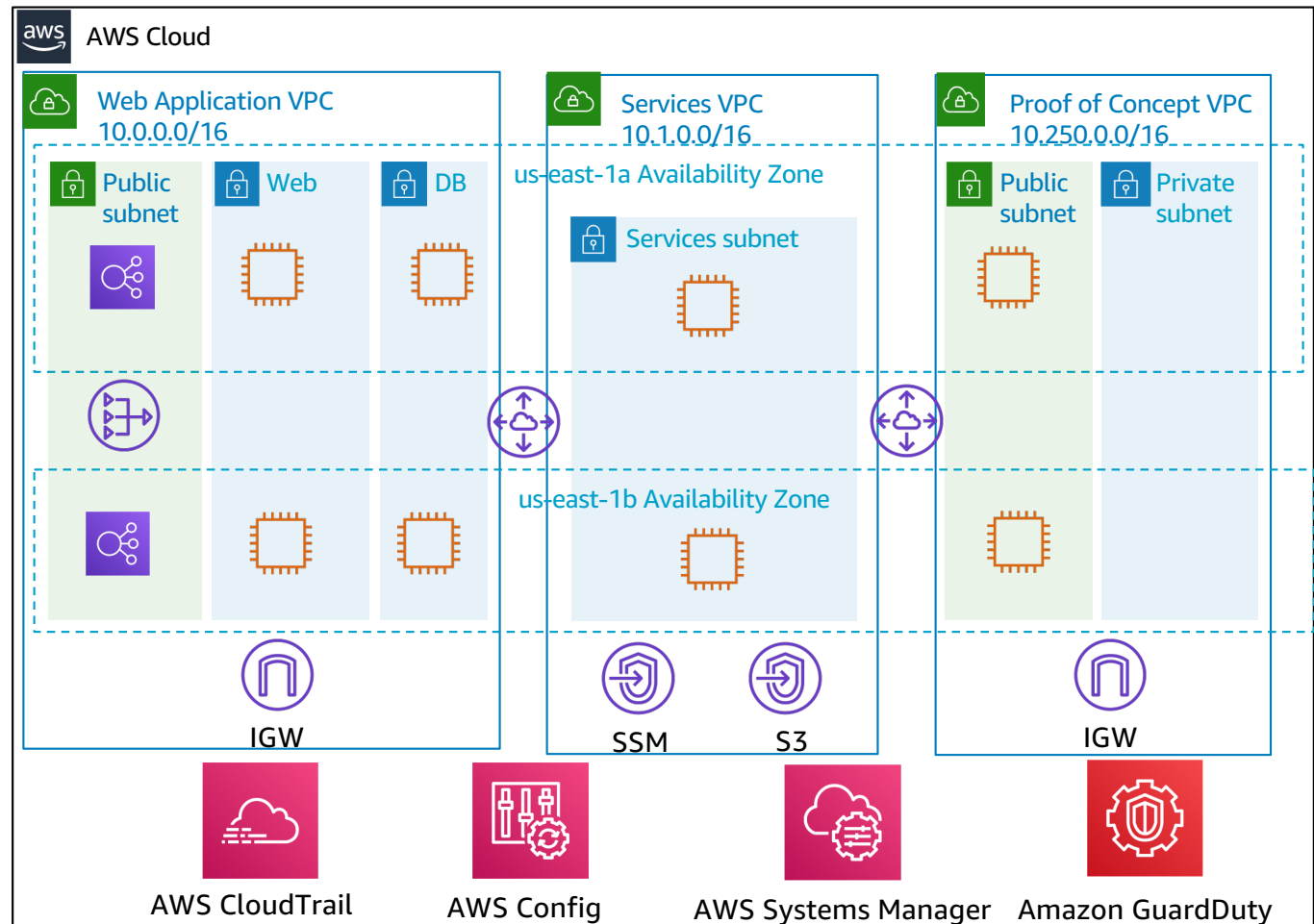
Isolation by default

- Easier & more restrictive

Secure insights across the board

New ways to secure access

- What if there was no SSH or RDP?













Let's Build!

<http://tiny.cc/reinforce-fnd203>

What did we learn?

- We can see everything going on in our AWS environment
- We have more granular, provable control of communications at a lower operational burden
- We can still explicitly deny access, but now in more places
- We have detailed logging and advanced monitoring of our control and data planes
- We can solve issues we never thought possible – like admin port risk

Let's not forget about partners

Host based security	Identity & access control	Configuration & vulnerability analysis	Logging & monitoring
 <p>ALERT LOGIC</p>  <p>ARMOR</p>  <p>SOPHOS</p>  <p>Symantec</p>  <p>TREND MICRO</p>	 <p>okta</p>  <p>oneLogin</p>  <p>PingIdentity</p> <p>Data protection</p>  <p>gemalto security to be free</p>  <p>Vormetric a Thales Company</p>	 <p>cavirin</p>  <p>CloudCheckr</p>  <p>CloudPassage</p>  <p>Dome9 SECURITY</p>  <p>evident.io</p>  <p>QUALYS Continuous Security</p>  <p>SAVIYNT</p>  <p>tenable</p>  <p>threat stack</p>  <p>TURBOT</p>	 <p>sumologic</p>  <p>splunk</p>  <p>ALIEN VAULT</p>