Let us know what you think

Click ‘engage’ to rate session.
Rate 12 sessions to get the supercool GOTO reward

Join the conversation #gotoldn
Google Inc., taking a new approach to enterprise security, is moving its corporate applications to the Internet. In doing so, the Internet giant is flipping common corporate security practice on its head, shifting away from the idea of a trusted internal corporate network secured by perimeter devices such as firewalls, in favor of a model where corporate data can be accessed from anywhere with the right device and user credentials.

The new model — called the BeyondCorp initiative — assumes that the internal network is as dangerous as the Internet.

(Wall Street Journal I “Google Moves Its Corporate Applications to the Internet” I May 11, 2015)
Setting the scene
Traditional apps

Business applications are *collections* of (virtual) *servers*

Database Tier

AppServer Tier

Web Tier

Is the “right” traffic going to/from our servers?

= type of server
Modern architectures don’t change things that much

Micro services based applications are **collections** of **services**

Persistence services

Business services

Front end services

= type of server

Is the “**right**” traffic going to/from our services?
Enterprise data centers are filled with these applications, often left insecure by lack of focus on interior network paths.

80% of Security Spend is on perimeter, 20% of traffic.
Hard on the outside, soft on the inside

Perimeter Security

Hacker Penetration
One penetration creates major “East-West” exposure

On average undetected for 234 days!
Cloud architectures have been different
2006 – The lonely (and exposed) VM
2008 - Overlays
2009 - VPCs
Containment often not enough – overlays stayed
Lots of people did something like this
Some even did something like this
And the really large (or paranoid) might do this
Or even this
Thankfully almost nobody tries to do this
What was that perimeter made of?

A quick detour to the worlds of:
Unified Threat Management

- Firewall
- NIDS/NIPS
- AV
- Anti Spam
- VPN
- DLP
- Load Balancer

UTM
Application Delivery Controllers

- Load Balancer
- Cache
- TLS offload
- Compression
- WAF
- Multiplexing
- Traffic Shaping
The UTM & ADC delivery model
SDN and NFV
Networks made from and configured by software

- **Network Function Virtualization**: Network is implemented through software.
- **Software Defined Networking**: Network is configured through software.
- **Open Flow**

Overlap: Software implemented network configured through software.
We can put a bunch of ‘network’ onto a VM

- Switch
- Router
- Firewall
- VPN
And add more functions into containers

Switch
Router
Firewall
VPN

NIDS/NIPS
Load Balancer
Cache
TLS offload
WAF

© 2015
This could be thought of as an app centric perimeter
But it refactors very readily into microservices
The audit paradox
Building in

CC photo by WorldSkills
Bolting on
PaaS gives us the chance to ‘bolt in’
But Docker adoption shows a movement against opinionated platforms
If a security event happens and it isn’t monitored
Some challenges remain
ToDo: SecDevOps

APIs are necessary but not sufficient: Need to have them integrated into the overall system.

Control metadata (and its mutability): Must be visible and understandable.

Security events need to be captured: Then turned into something humans can action.
Please remember to rate this session. Thank you!
Thanks!