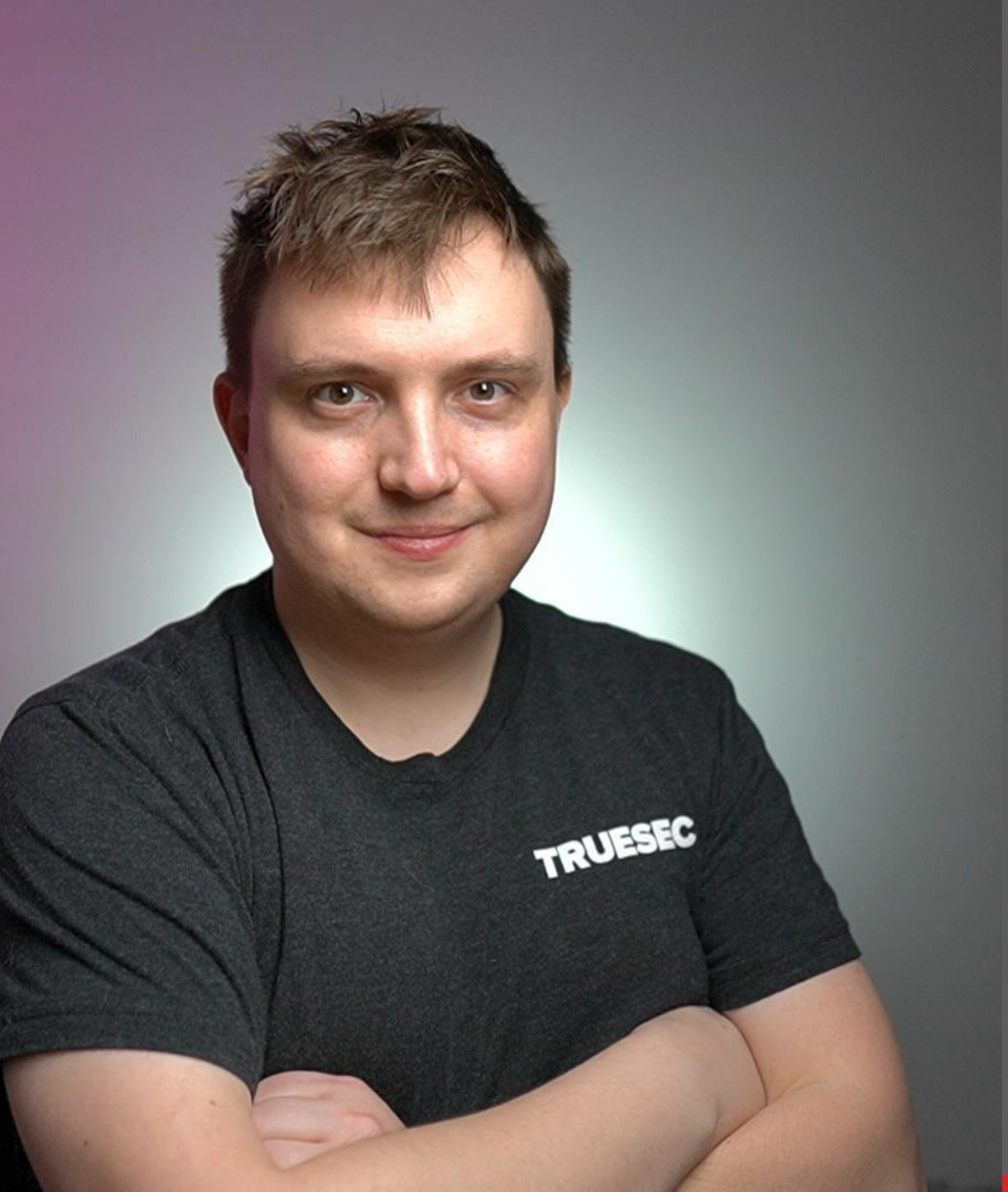
PATCHING IN A REMOTE WORLD

The three scenarios – ish.



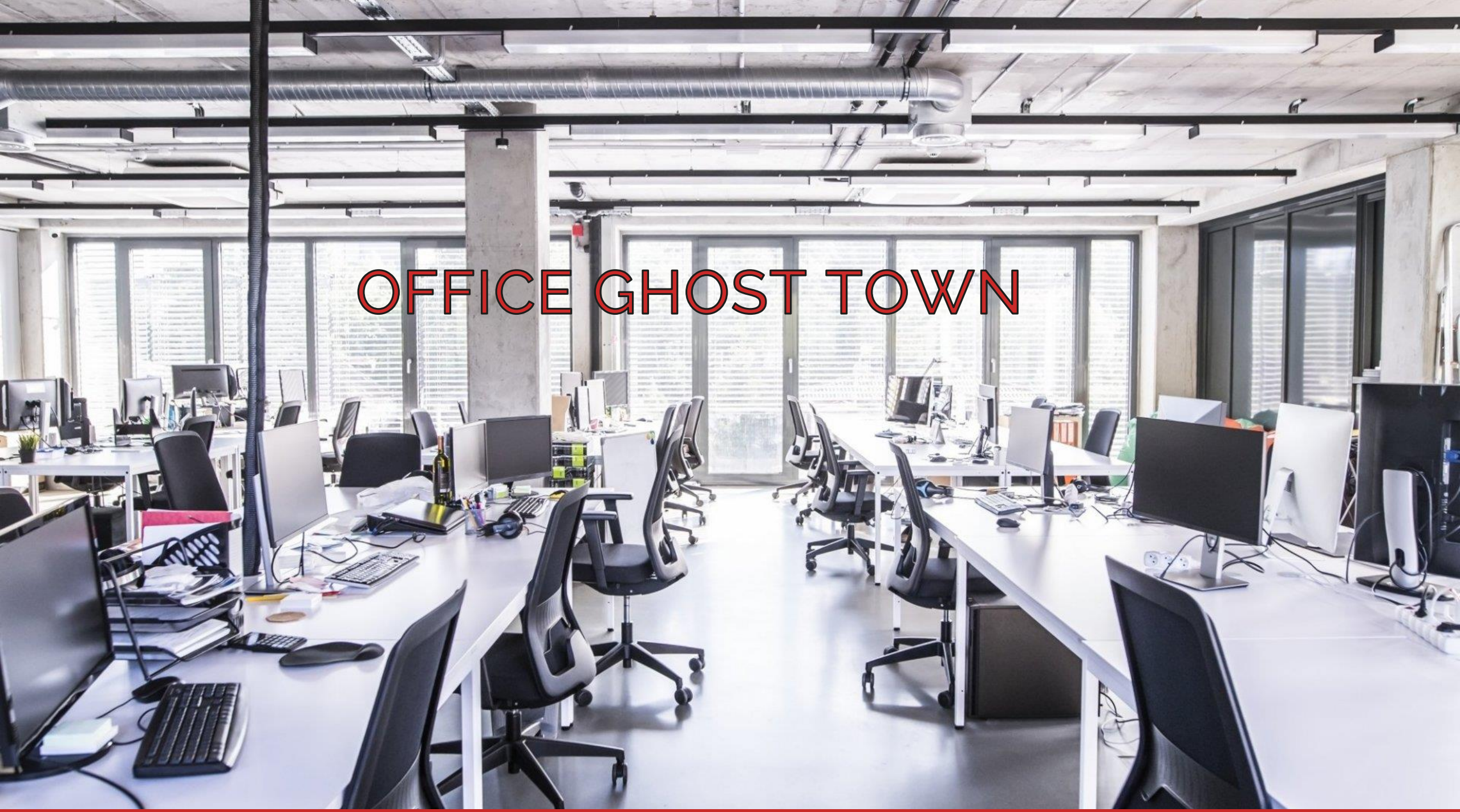
JORDAN BENZING

Senior Consultant @Truesec

- Cyber Security Incident Response
- Worked in IT since 2008
- WinAdmins Discord Admin
- Official Ramen Eater

@JordanTheITGuy

Jordan Benzing | LinkedIn


OFFICE GHOST TOWN

PATCH MANAGEMENT – C19 SCENARIOS

The Prepared

- Cloud Native Organizations
- Organizations who have a way to monitor, and manage remote devices regardless of network.

The Almost Ready

- Organizations who can manage remote devices sometimes

The Now What

- Companies with no management.
- Companies who have experienced a security incident.

PREPARED ORGANIZATIONS

Intune Only

- No on-prem infrastructure
- Devices always managed
  - * As long as there is Internet
- Feature Updates Probably Easy

Cloud Management Gateway

- Devices always managed
  - * As long as there is Internet
- On-Prem Infrastructure
- Cost Associated
  - More on that later….

Co-Management

- Devices Always managed
  - For specific things
- Easy to set up
- Requires on prem infrastructure
- Easiest to migrate to

COMPANIES A YEAR AGO – OR TODAY

Scenario One

- MEMCM is installed
- Always on VPN Preserves Line of Sight

Scenario Two

- MEMCM Installed
- User initiated VPN

Scenario Three

- MEMCM is Installed
- No VPN available
- Devices are registered
- Intune Rings aren’t allowed
  - (For ‘Reasons’)

CONFIGURING CO-MANAGEMENT

In five minutes (Sounds like youtube video)

NOW WHAT?

Intune Update Rings

- Co-Management & Intune Only customers both use this solution
- Can Pause Updates if something goes wrong
- Can Roll-Back Updates if something goes wrong
- Scheduling is based on patch release
- Has the ability to natively apply Feature Updates
- Reporting is… Different

ONE RING TO RULE THEM ALL

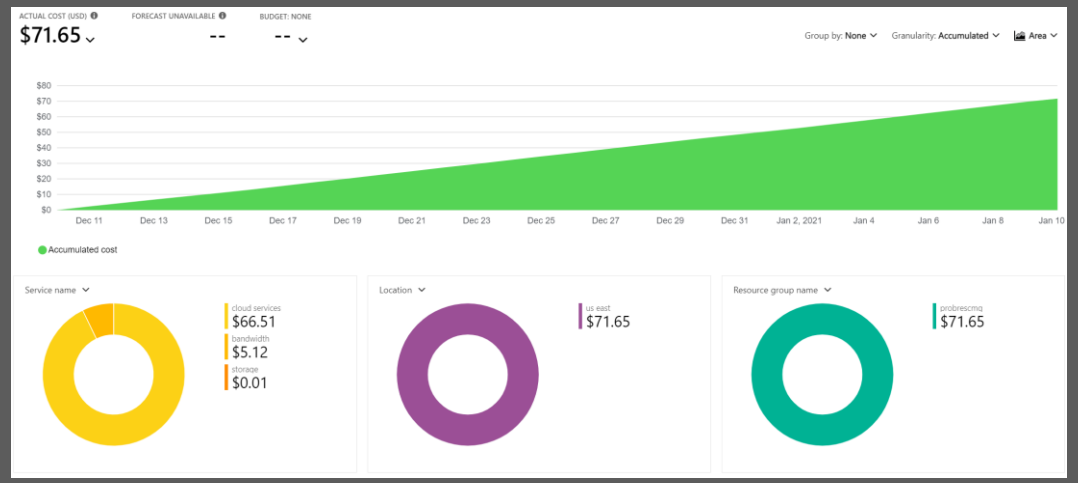
Windows Update Rings - Intune

CLOUD MANAGEMENT GATEWAY

- Standard patching just like On - Prem
- Allow downloads from different locations as told
- Some Granular Patching Options
- Allows the full Configuration Manager Feature Set

SHOW ME THE MONEY

- Obtain Certificate – Price $0.00 -> $150 -> Infinity and beyond
- Configure your Azure Subscription for the CMG Application – Price $0.00
- Create an Azure Service Connection – Price $0.00
  - This creates your applications
- Create the CMG and provide Authentication path – Price (~$70 - 90 Monthly)
- Install The Connection Point – Price 0.00
- Configure the MP for the CMG
- Configure the SUP for the CMG
- Configure Client Settings
- Deploy Patches



DEPLOYMENT TRICKS

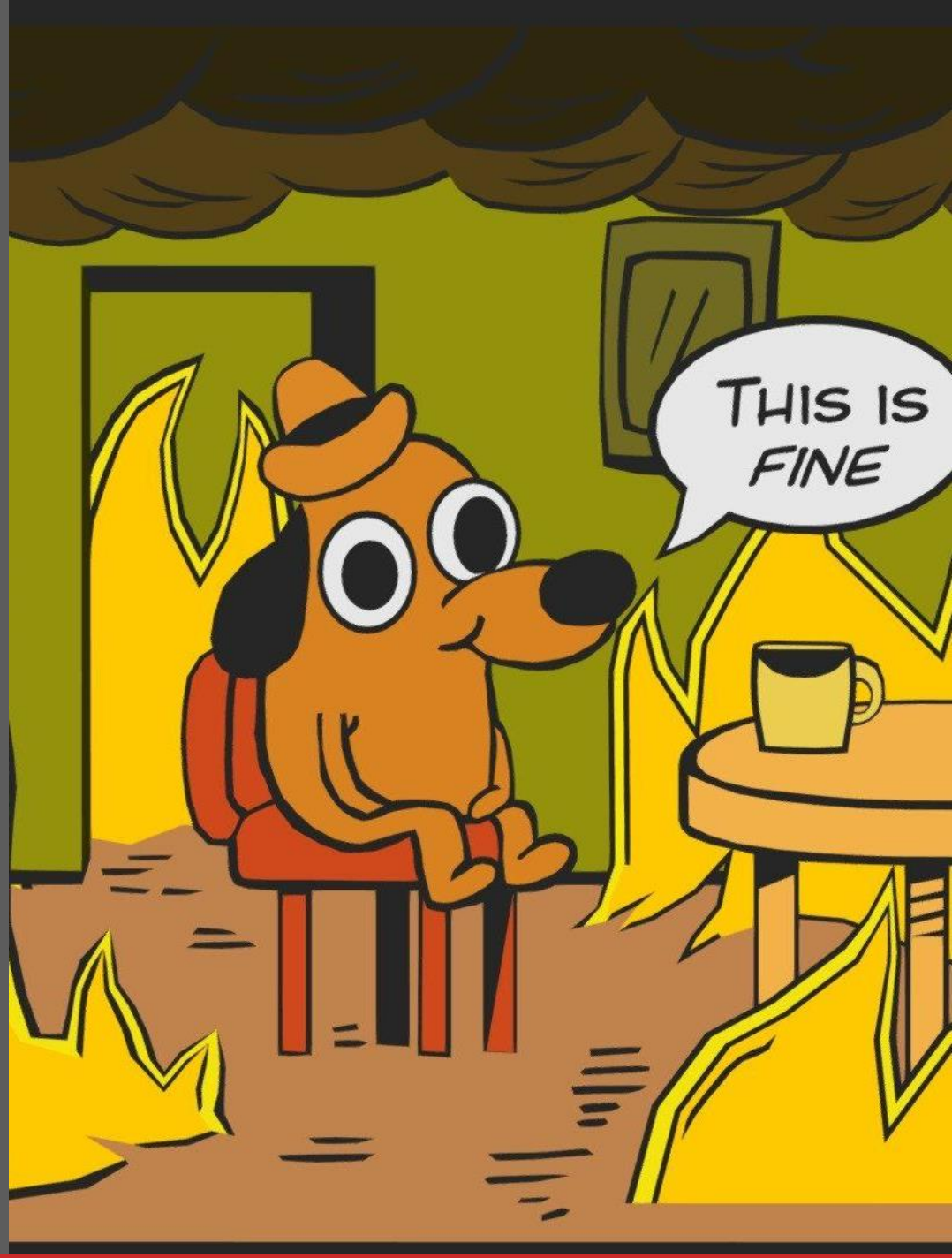
Tips and Tricks for Update Deployment

CAN YOU DO IT CHEAPER?

- Configure Co-Management – Price $0.00
- Configure Tenant Attach (Bonus Points) – Price $0.00
- Validate Client Settings are properly configured – Price $0.00
- Deploy Co-Management Settings to all devices connecting via VPN – Price $0.00
- Enroll devices in Intune – Price $0.00
- Enroll Deploy Patch Rings and enjoy

Now What – Incident World

- Computers Went Home (No VPN No Contact)
- Security “Event” – Now What?
  - Cloud Based Re-image (Auto-Enroll)
  - Straight to Chicken – But what if you can’t?
  - Build On-Prem VPN Server
  - Deploy Certificate to clients with Intune
  - Deploy ConfigMgr Agent
  - Continue as Needed



REPORTING OF LAST RESORT – ATP/API

If you've onboarded devices…