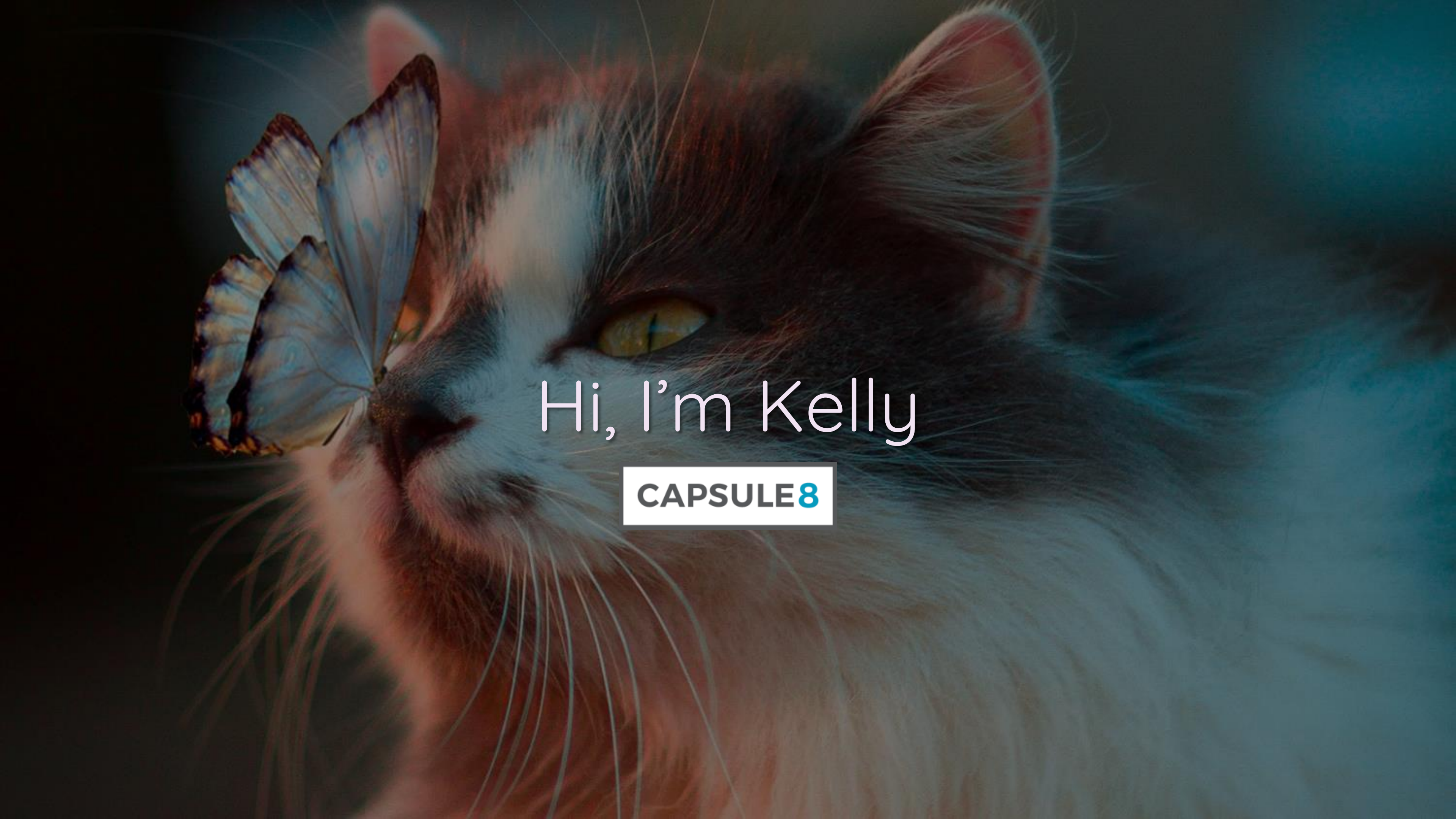
Security Delusions

Kelly Shortridge (@swagitda_)

QCon NYC 2019

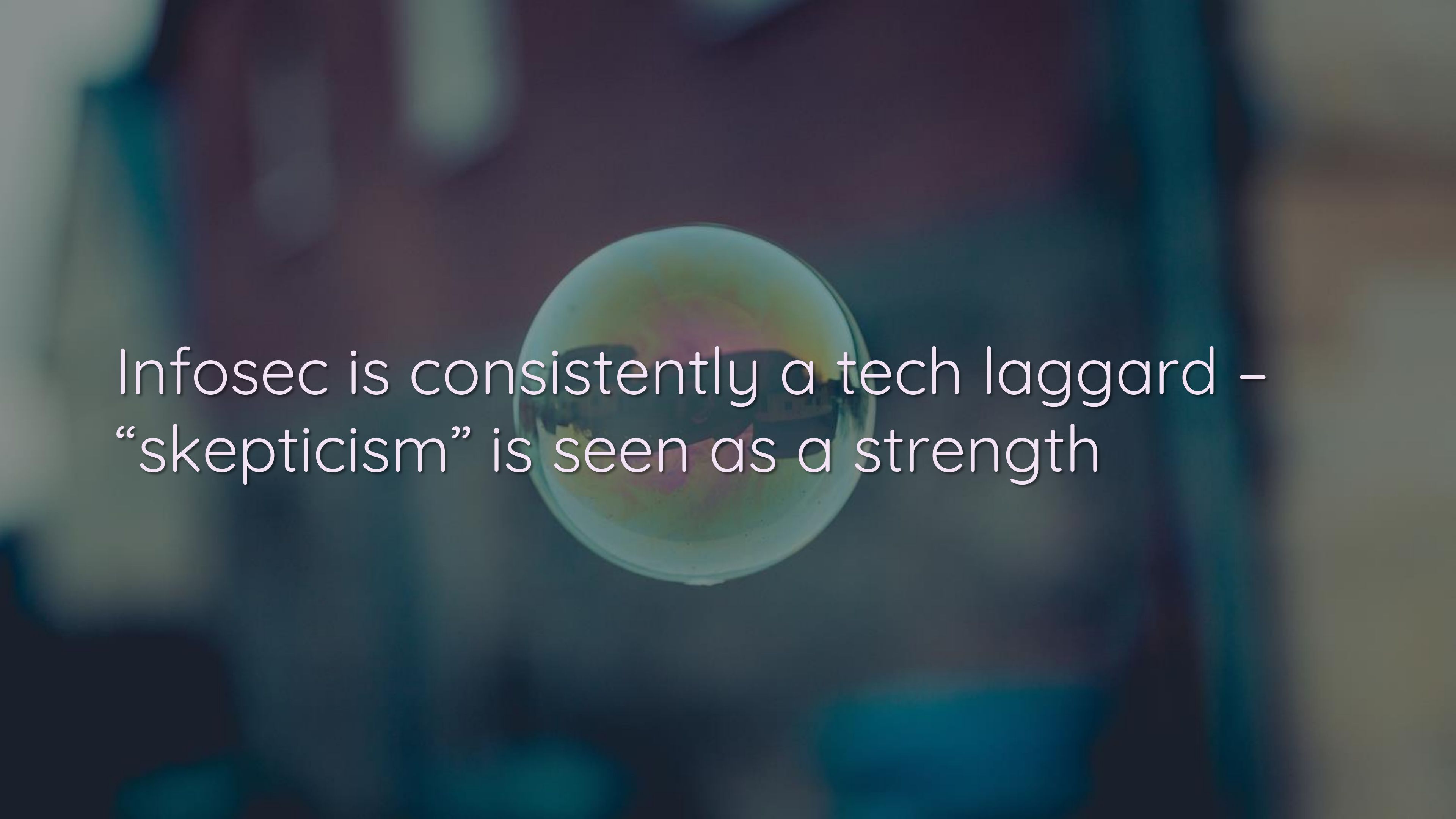


Hi, I’m Kelly

CAPSULE8

“Ignorance is the parent of fear.”

— Herman Melville, *Moby Dick*



Infosec is consistently a tech laggard –
“skepticism” is seen as a strength

How can you herd these frightened sheep to modern tech pastures?

1. A History of Cloud Compunction
2. APIs: Infosec’s Anathema
3. The Curse of Containers
4. Cheat Codes for Dealing with This

A History of Cloud Compunction

“Cloud transformation” ruffled infosec feathers in the early 2010s

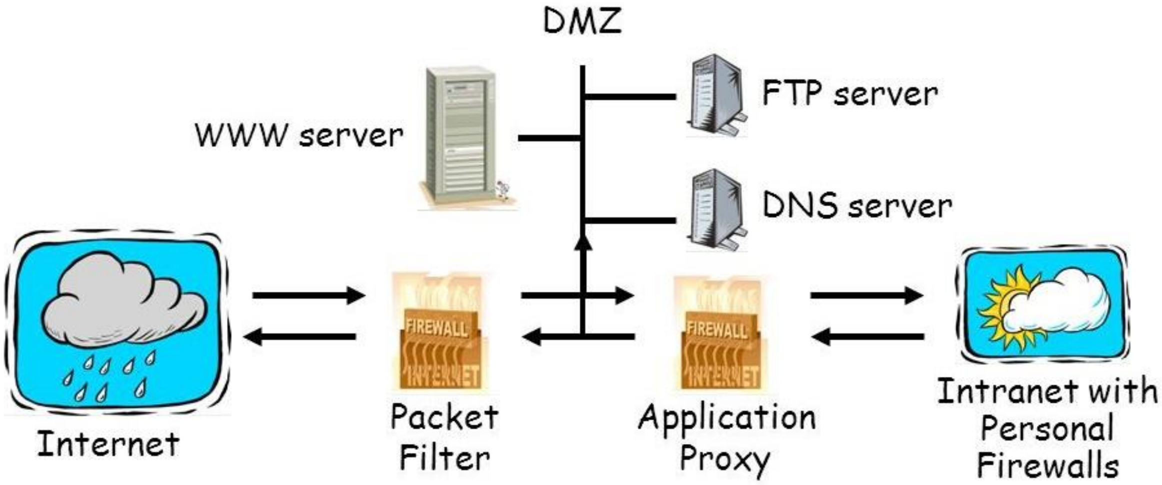
“Storing data online,” shared resources, insider threat, DDoS, supply chain…

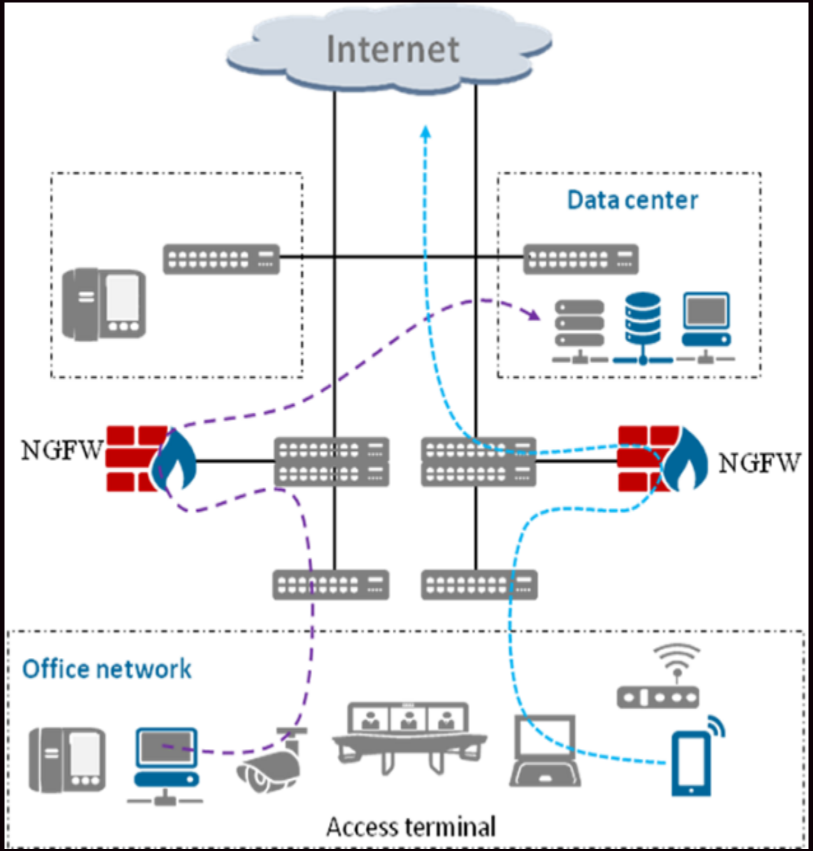
The crux of cloud fear was rooted in a loss of control by the infosec team

The firewall was always the center of the enterprise infosec universe

Firewalls and Defense in Depth

- Example security architecture



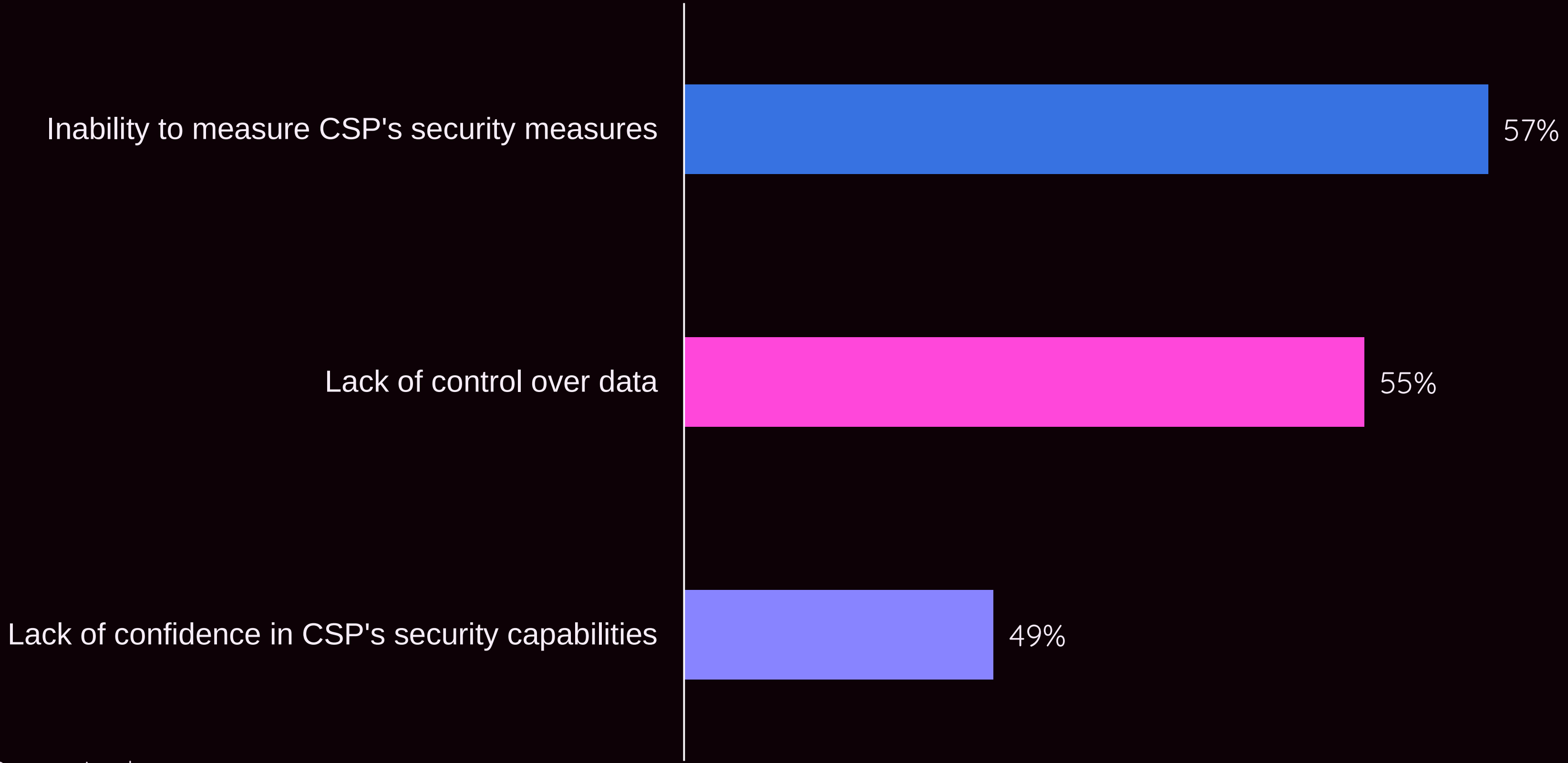

Internet
Data center
NGFW
NGFW
Office network
Access terminal

Defense in Depth model: the firewall is the first line of defense

Cloud + microservices represents a Copernican revolution for infosec

What do surveys from yesteryear reveal about infosec's fear of cloud tech?

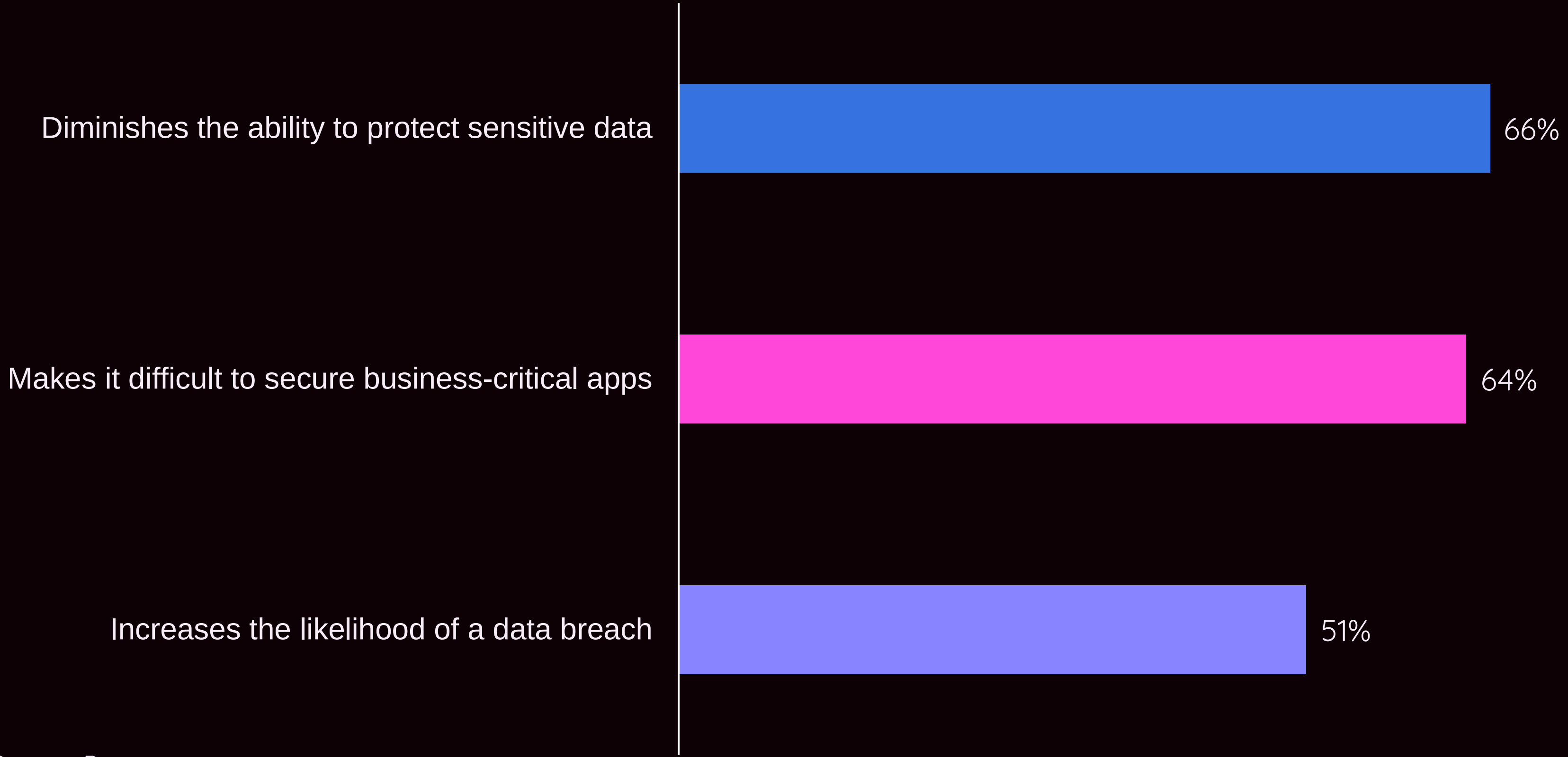
2012: “What is holding back cloud?”



Source: Intel

“Uneasiness about adequate firewalling”
= the pre-Copernican mindset

2014: Cloud Multiplier effect on security



Source: Ponemon

2015: 71% view cloud data security as a big red flag & 38% feared loss of control

Source: Cloud Security Alliance

Endowment effect & sunk cost fallacy:
“Our security is better than CSPs!”

Evidence is quite scant that CSPs are breached more frequently

Acceptance that CSPs have better security is only in the past few years

Reality: misconfigurations are the biggest concern for cloud security

Gartner: “Through 2020, 80% of cloud breaches will be due to misconfiguration … not cloud provider vulnerabilities”

Using cloud-native security controls can reduce security expense by 30%

Source: McKinsey

Network security blinky boxes often carry price tags of $100k - $200k

So, how is infosec reacting to emerging tech today?

APIs: Infosec’s Anathema

Microservices fears: APIs + containers

Horror story: microservices creates a titanic, labyrinthian attack surface

Basically monolithic app risk x 10,000 = infosec’s mental model of microservices

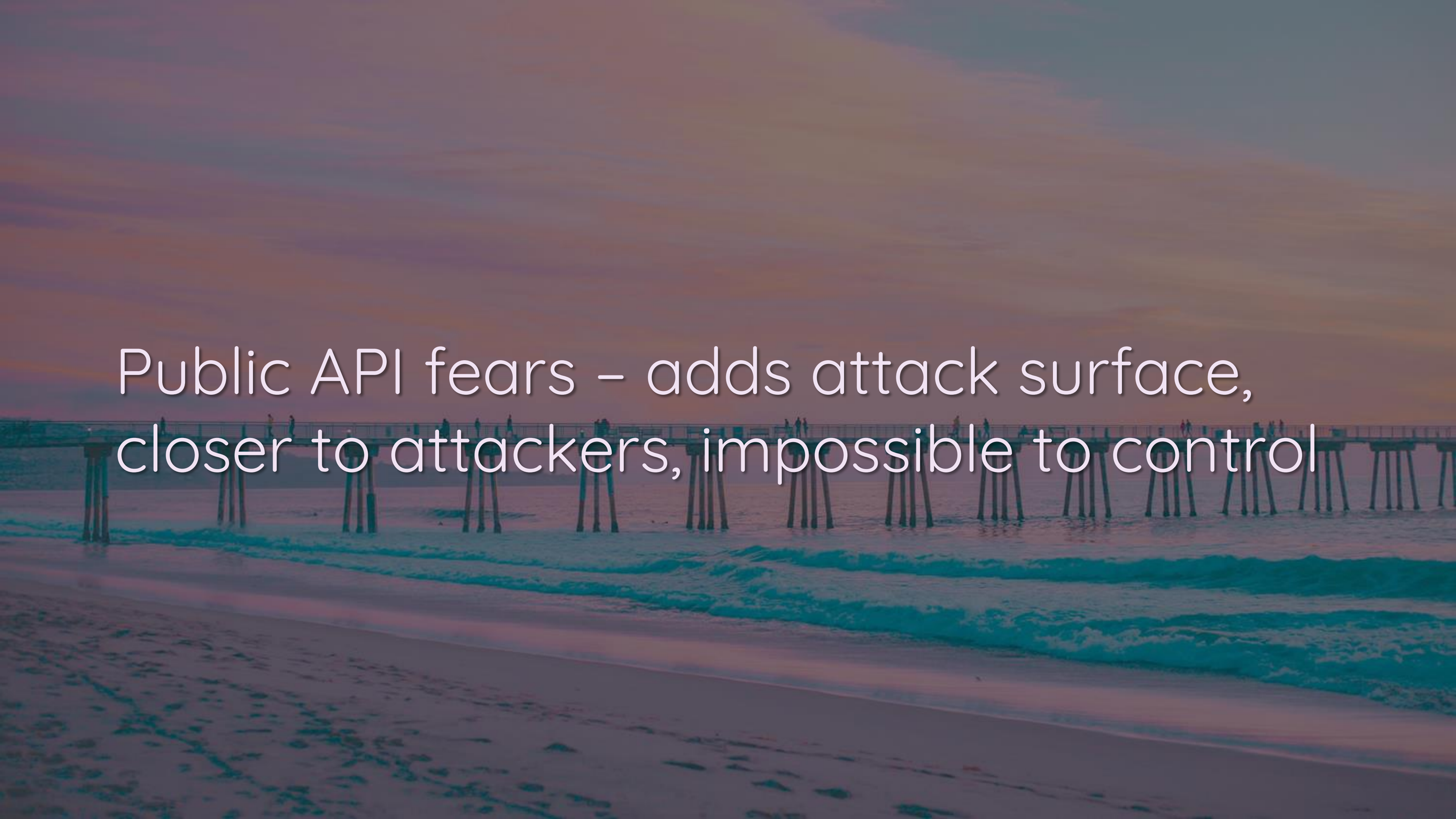
Revisionist history: as long as the perimeter is secure, the org is safe

Real history: lateral movement was easy because everything else was #yolosec

Public-by-default begets embedded security vs. bolt-on security – a big win

2018: 51% aren’t certain the infosec team knows all APIs within the organization

Source: Ping Identity



Public API fears – adds attack surface, closer to attackers, impossible to control

A lie: “Formerly, local networks had only a few connections to the outside world, & securing those endpoints was sufficient.”

Public API fears – provides a “roadmap” for underlying functionality of the app

Reality: “Security through obscurity” is a garbage cop-out

Security resilience: assume your added security controls will fail

API endpoints actually raise the cost of attack – attack tools don’t work & entire vuln classes are removed

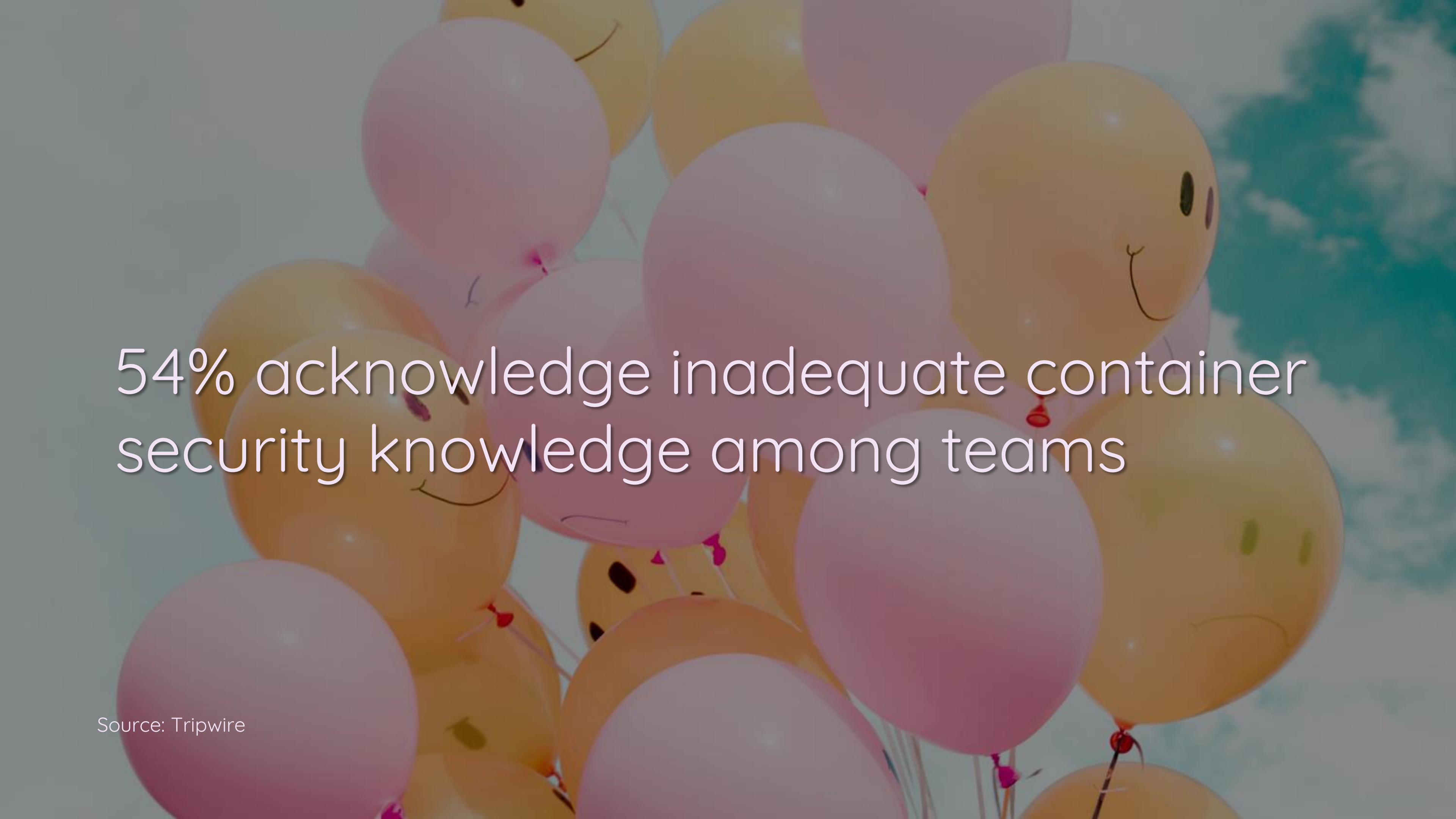
Standardization begets security benefits – but isn’t a common concept in infosec

The Curse of Containers

Few in infosec realize containers aren’t just featherweight VMs

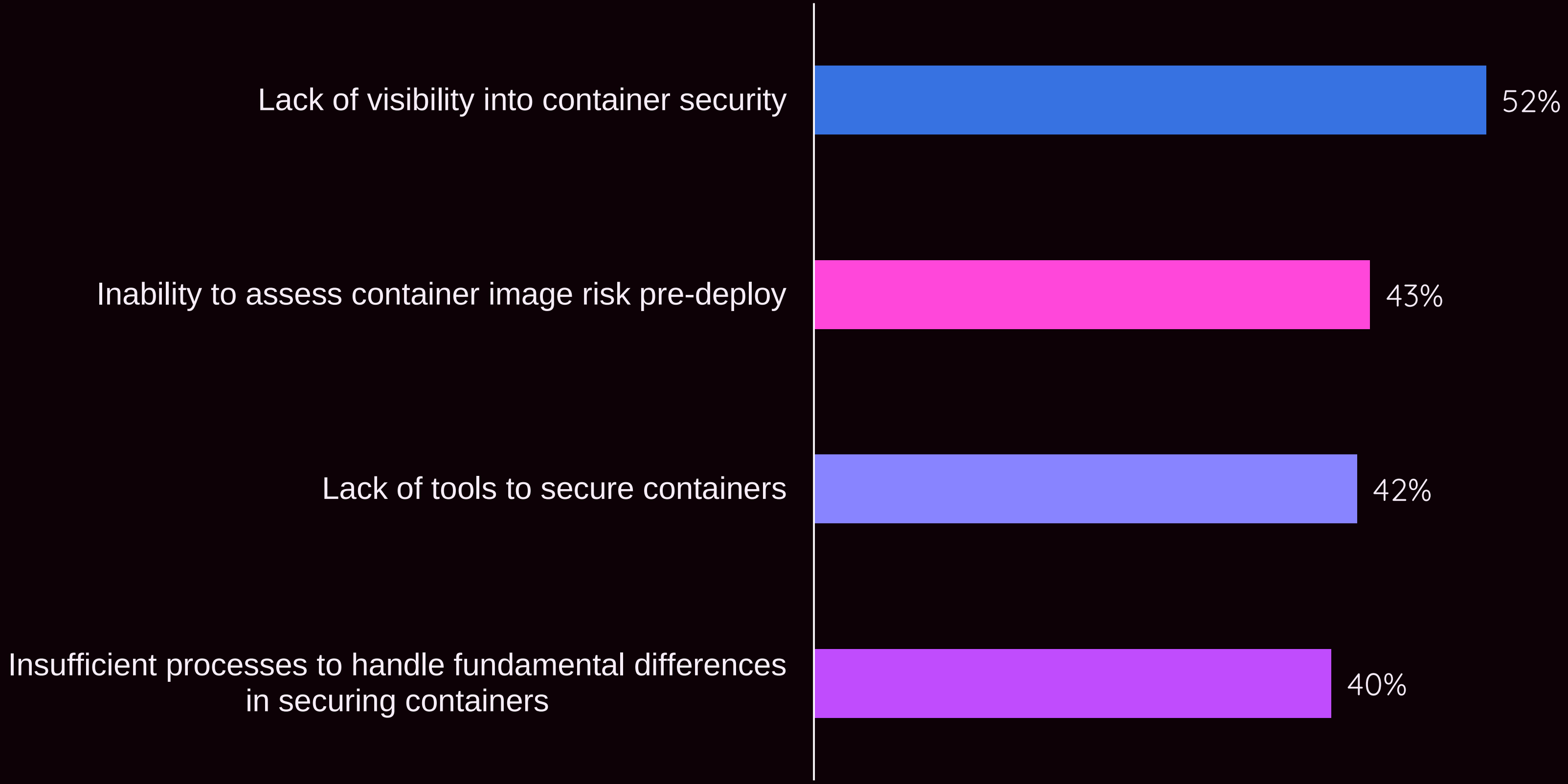
2019: 94% have concerns on container security – leading 42% to delay adoption

Source: Tripwire



54% acknowledge inadequate container security knowledge among teams

Source: Tripwire



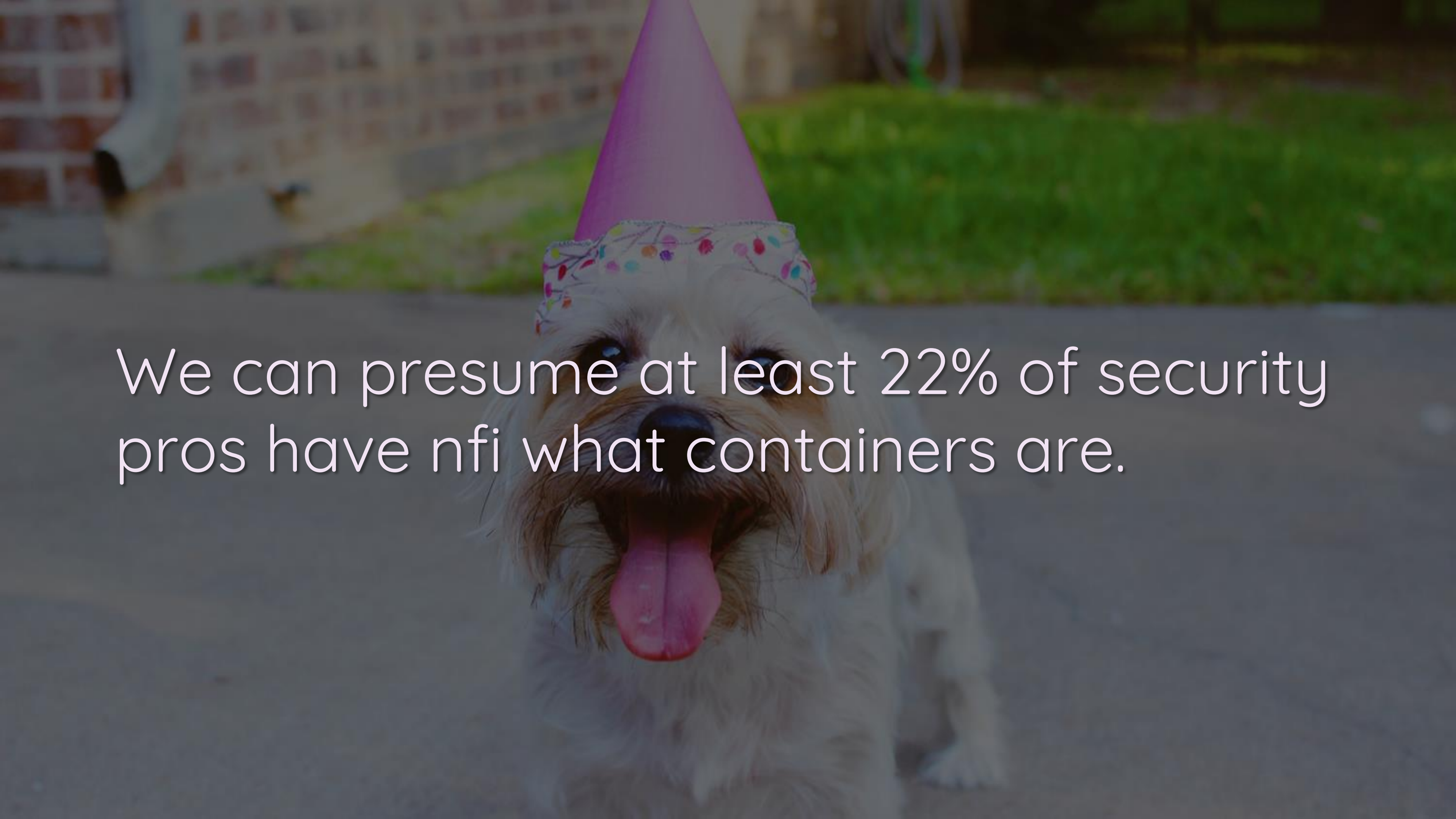
Source: Tripwire

52% want incident detection & response.
49% want isolation of pwned containers.

Source: Tripwire

40% want “AI security analytics” & 22% want “blockchain” to secure containers.

Source: Tripwire



We can presume at least 22% of security pros have nfi what containers are.

Straw man: each container needs its own monitoring, management, & securing

Standardization fear: vulns can be replicated ad infinitum

Because scanning for vulns in monolithic, custom-built Java apps is easy???

Rose-tinted glasses: monolithic apps = “You know exactly where the bad guys are going to try to get in”

Microservices: easily mapped workflows means easier threat models

Container fear: shared environments (just like with cloud previously)

Should we go back to apps talking over FTP, telnet, SSH, random UDP ports, etc.?

Past: get in via a running FTP service

Containers: exploit the web server

Container fear: too easy for devs to use vulnerable versions of software

As opposed to what – versions of Windows Server 2008 with Metasploit backdoors ready to go?

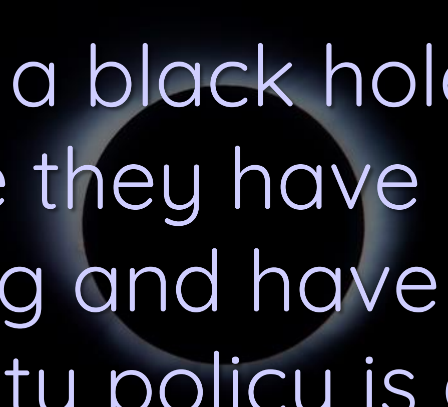
Separating complex functionality into separate services is better for security

Now that we’ve explored the tinfoil universe, how do we return to reality?

Cheat Codes for Dealing with This Mess

How can we evangelize real threat models & solutions in this new world?

Warning: Infosec largely views DevOps as a frenemy (at best)



“DevOps is like a black hole to security teams because they have no idea what DevOps is doing and have no way of ensuring security policy is enforced.”

Telling someone gripped by fear to “calm down” will backfire

Acknowledge there are relevant concerns for using this tech – just not the ones they believe

Which concerns should you highlight? There are three critical basics:

1. Don’t expose cloud storage publicly
2. Don’t use unauthenticated APIs
3. Don’t use “god mode” in containers

Infosec’s job becomes validating adherence to established best practices

Analogize “new security” to pre-Copernican methods to facilitate comms

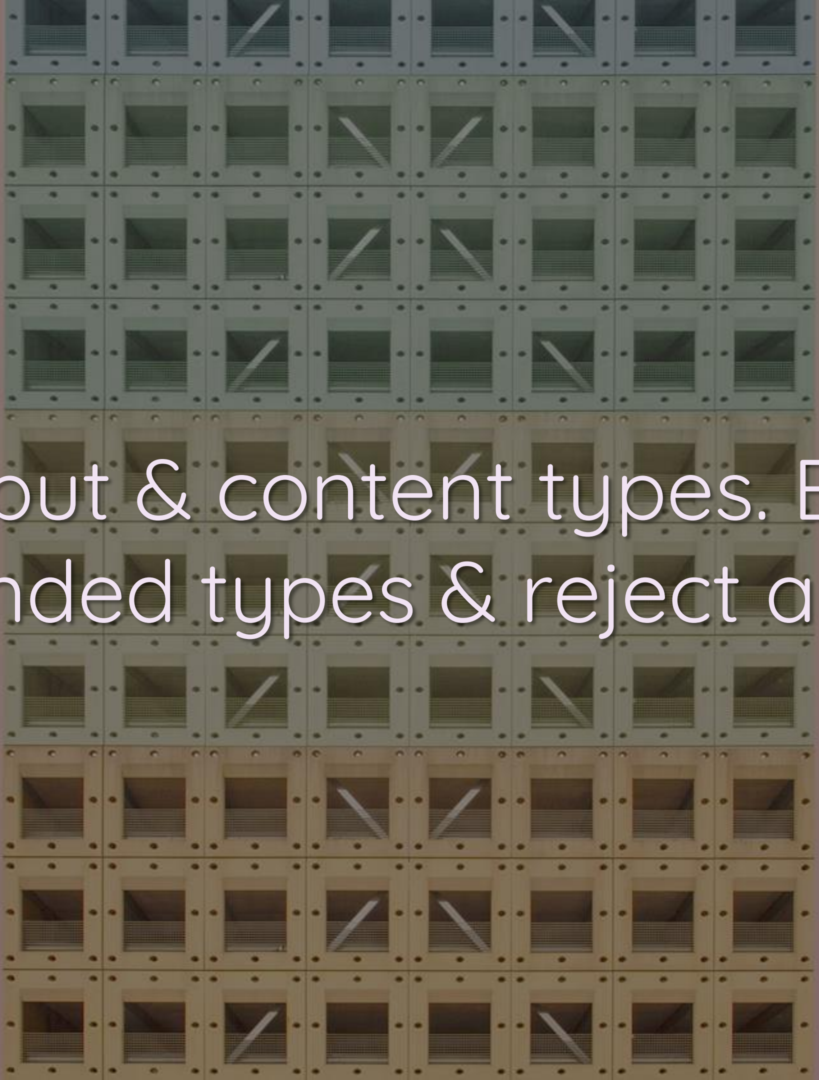
Example: security groups & network isolation by CSPs = firewall equivalent

Amazon Inspector + AWS Trusted Advisor are great tools to start

Use IAM roles for least priv or segment prod + dev through different accounts

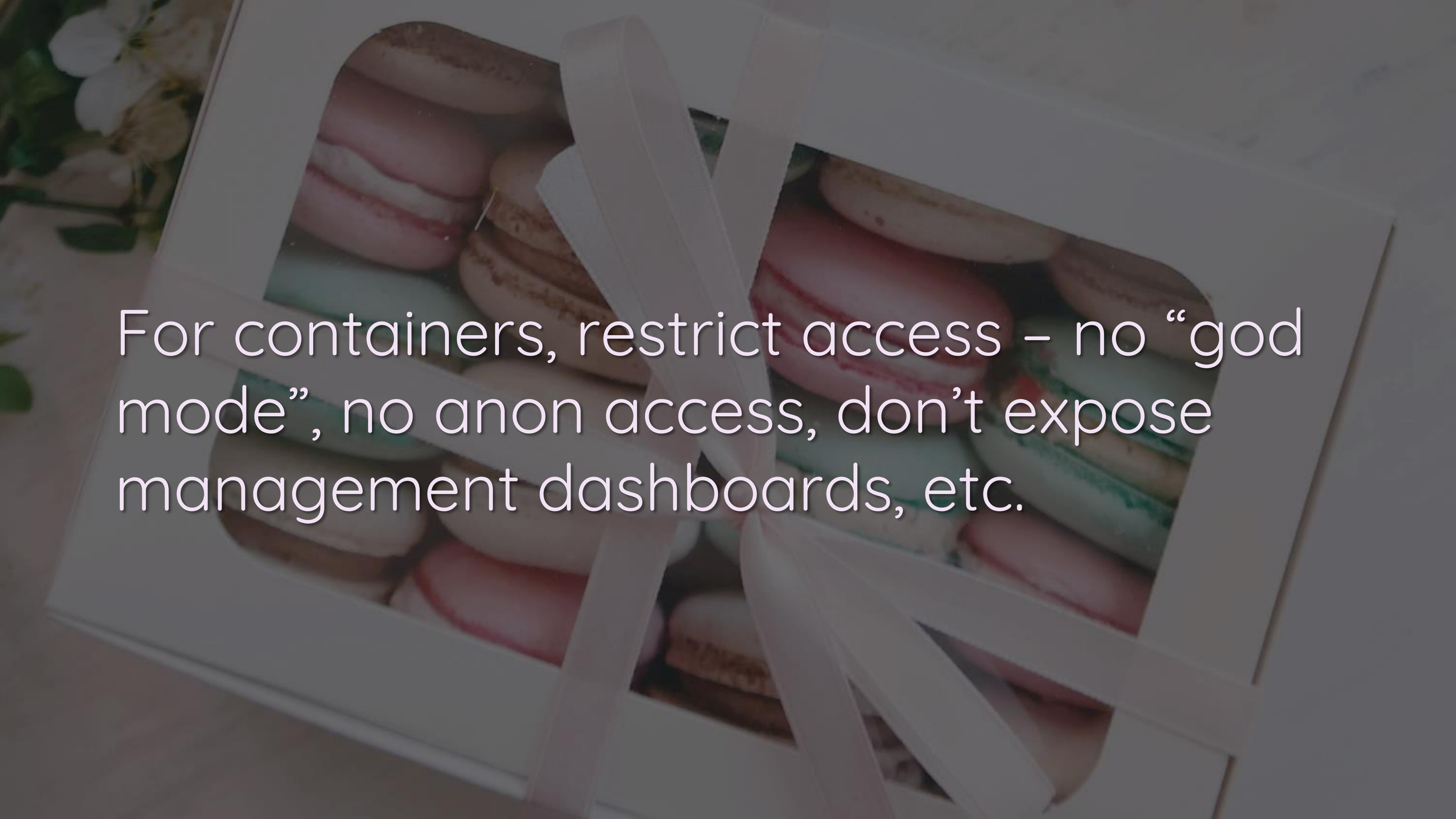
Basic API hygiene will suffice – auth, validation, & not trusting external data

Example: Don’t expose API keys in the URL, only use HTTPS endpoints, etc.



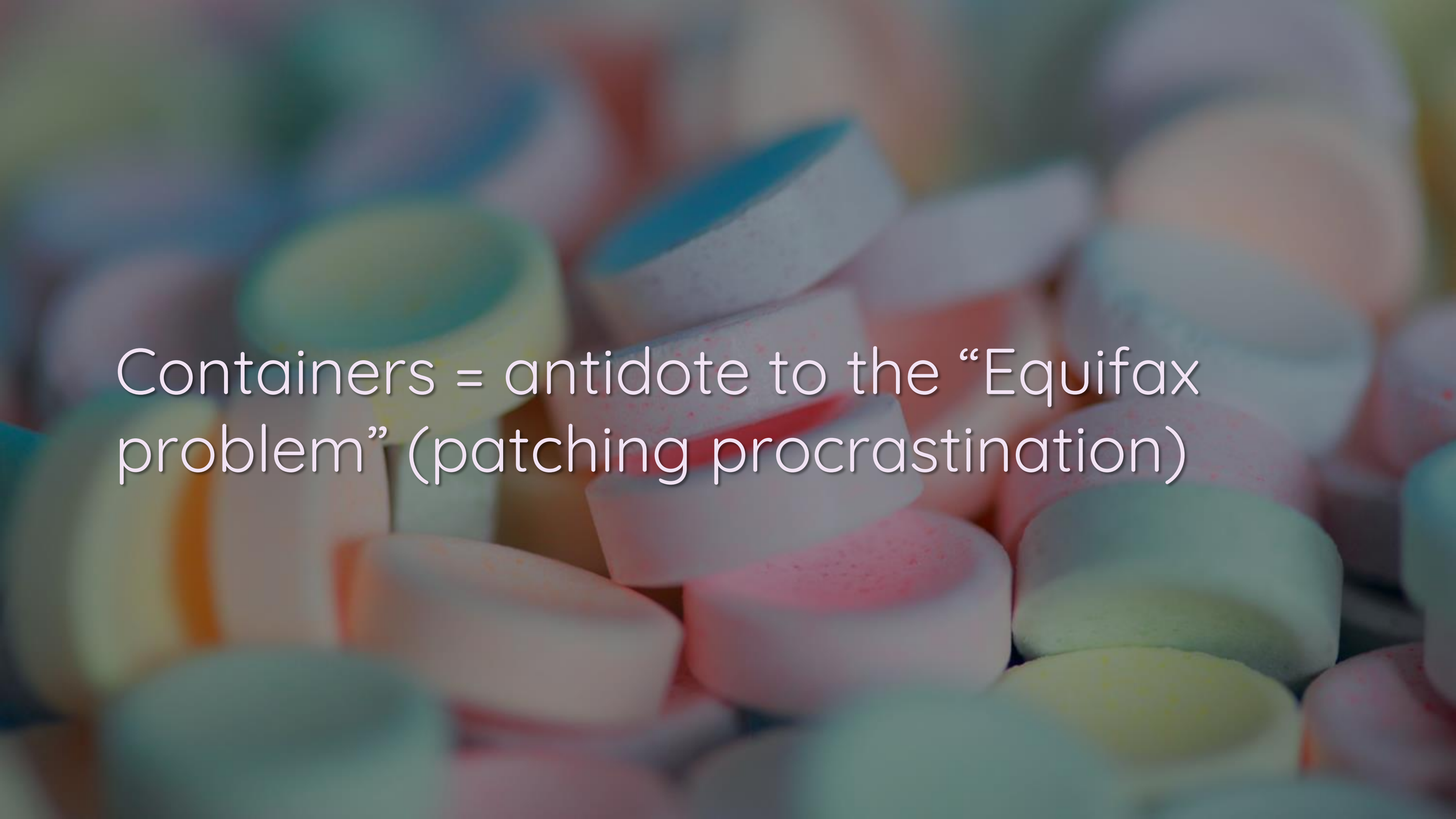
Validate input & content types. Explicitly define intended types & reject all others.

Analogize this as a form of granular whitelisting only possible with APIs



For containers, restrict access – no “god mode”, no anon access, don’t expose management dashboards, etc.

Any CISO will already be familiar with the concept of “Least Privilege”



Containers = antidote to the “Equifax problem” (patching procrastination)

Container registries make security scanning easier & add sense of control

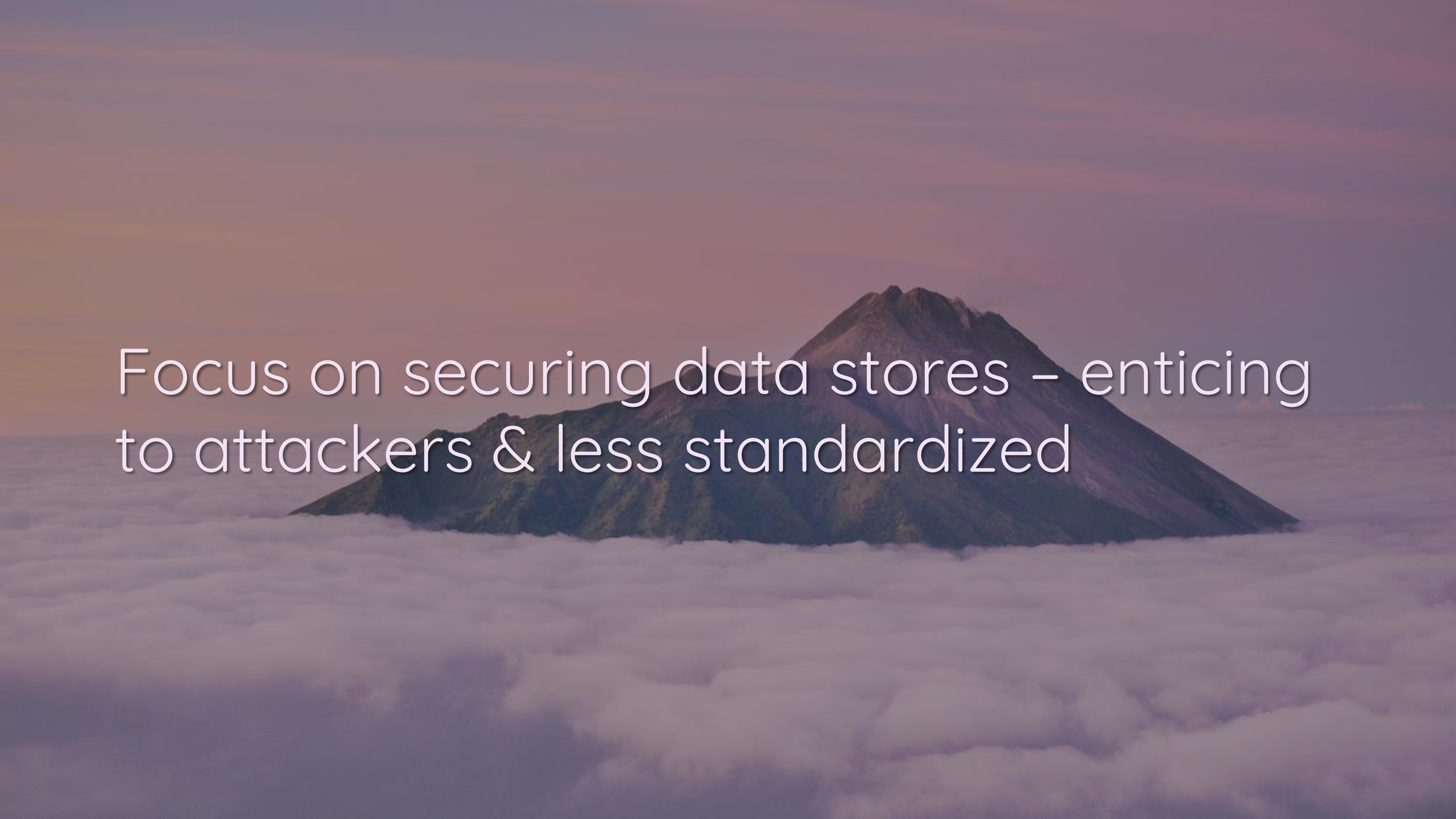
Live migration means security can patch without impacting end users

Analogy: Windows updates if Word & PPT docs were migrated to a healthy OS

If misconfigs are covered, what remains for infosec teams to tackle?

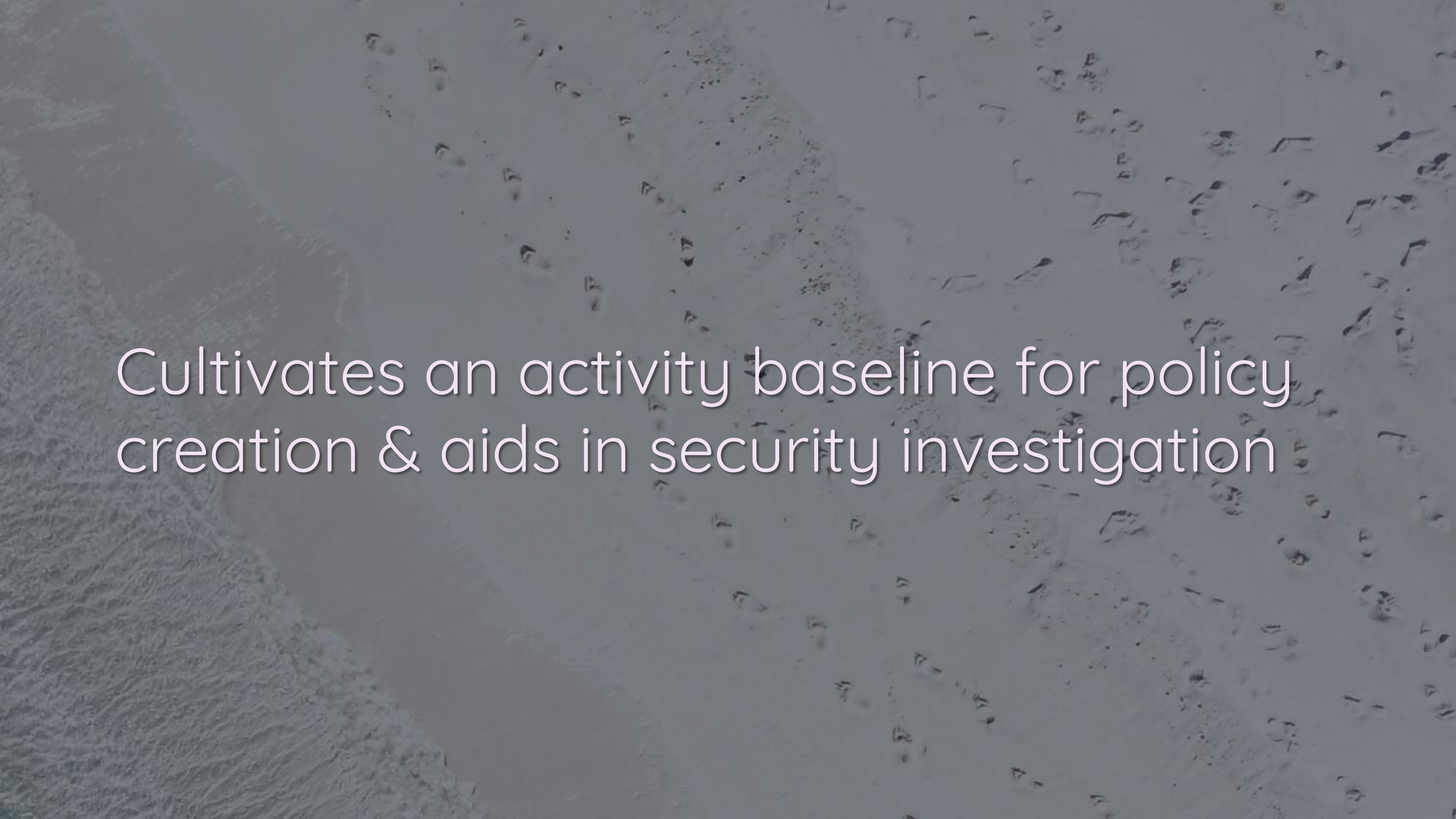
Codifying secure configs – modern equivalent of security policy templates

Documenting threat models, starting with scenarios most damaging to the org & working back to likely vectors



Focus on securing data stores – enticing to attackers & less standardized

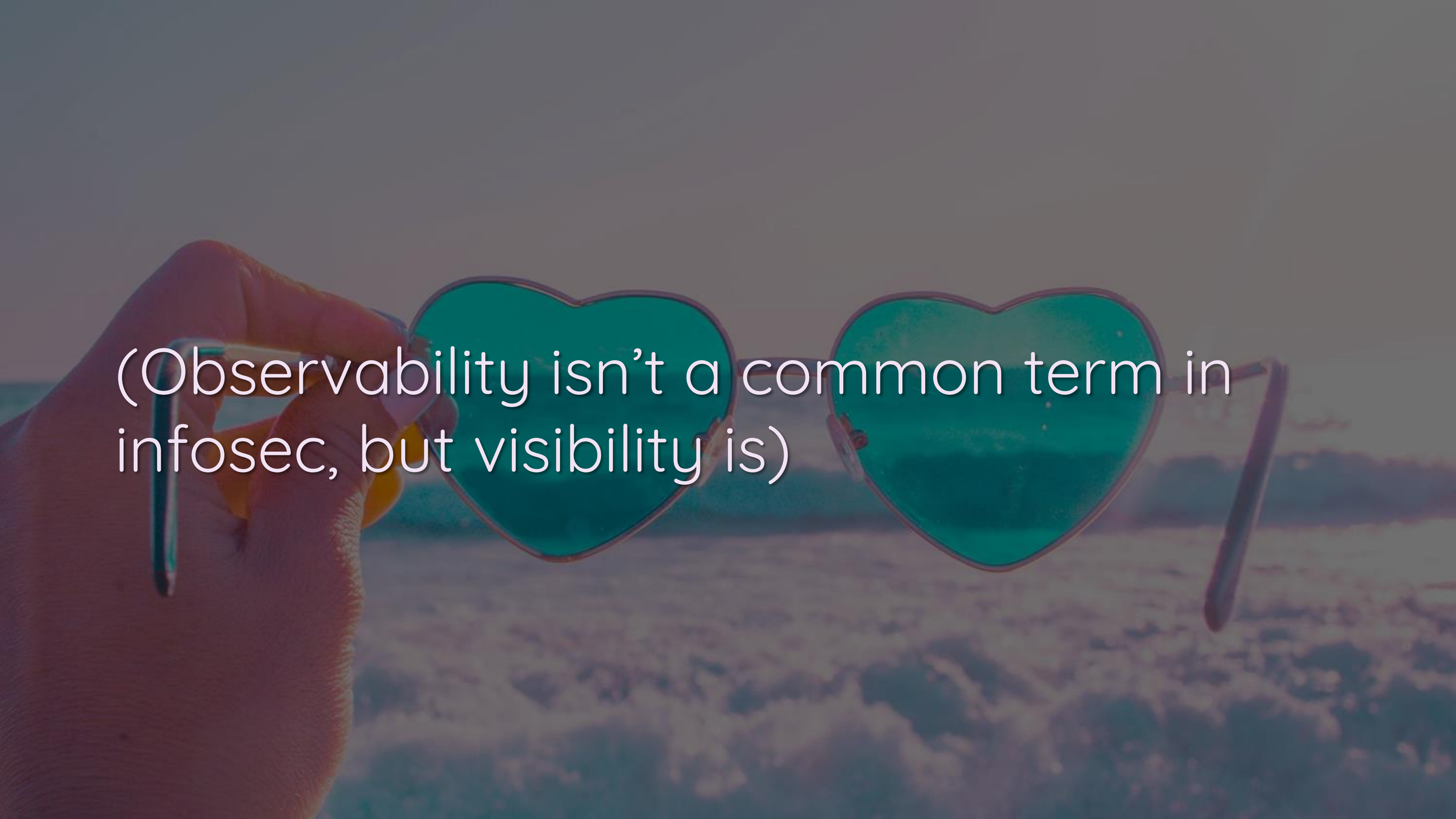
Help infosec finds database visibility & monitoring tools (e.g. Vivid Cortex)



Cultivates an activity baseline for policy creation & aids in security investigation

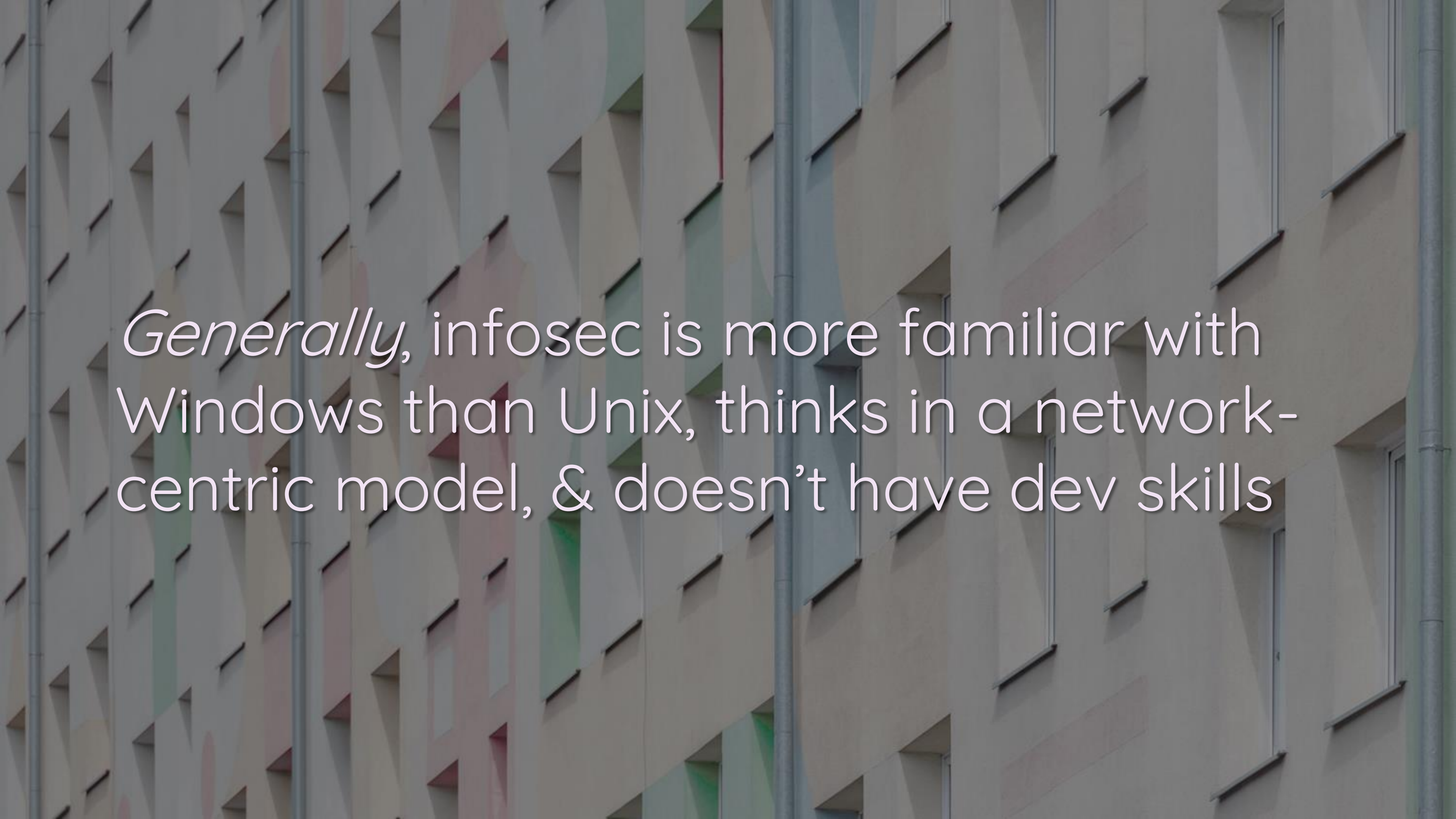
Highlight compliance – file integrity monitoring underpins most standards

FIM is easier given the improved inspectability of containers

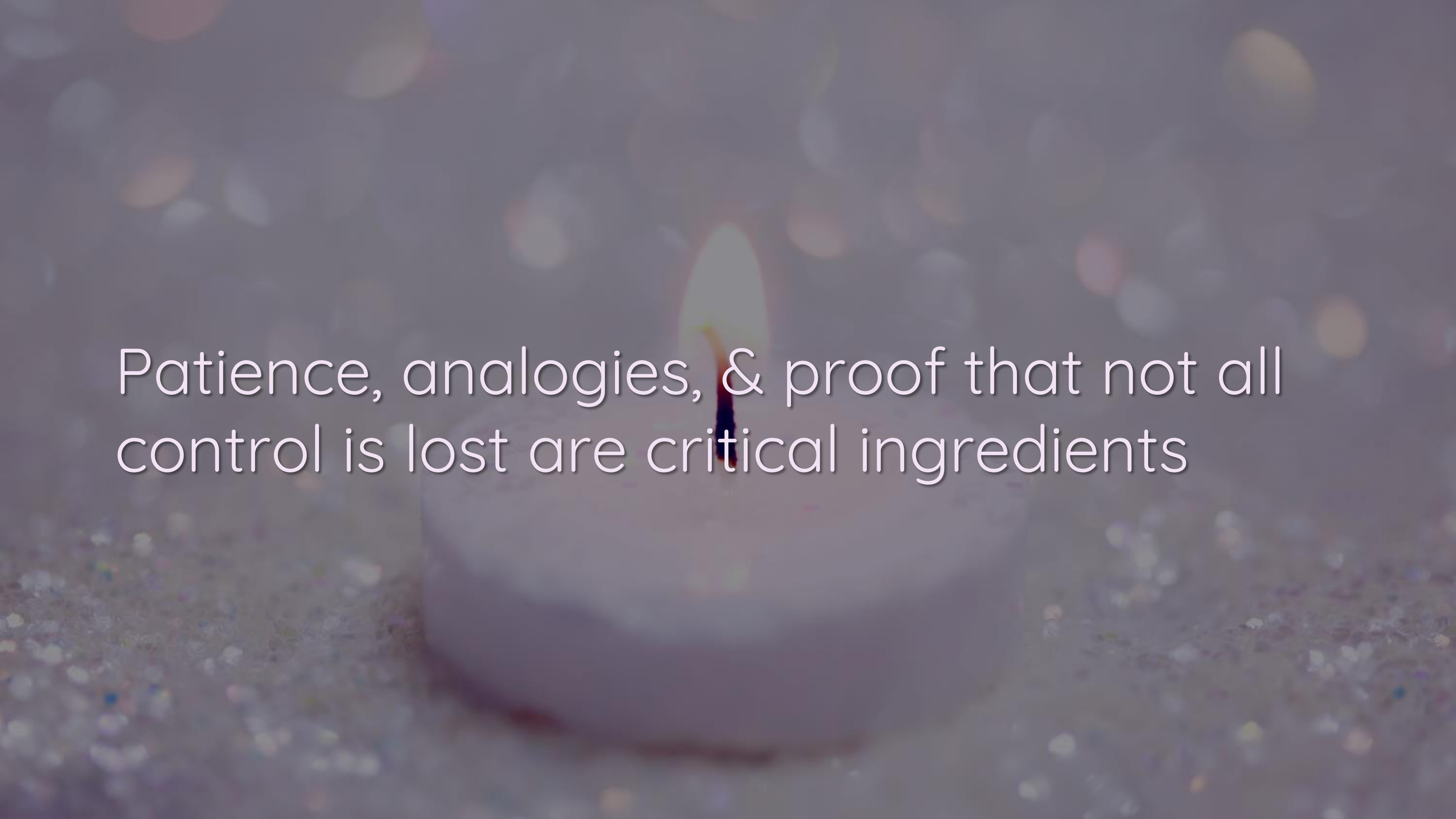


(Observability isn’t a common term in infosec, but visibility is)

Infosec ppl aren’t all the same – different tactics will work to build understanding



Generally, infosec is more familiar with Windows than Unix, thinks in a network-centric model, & doesn’t have dev skills



Patience, analogies, & proof that not all control is lost are critical ingredients

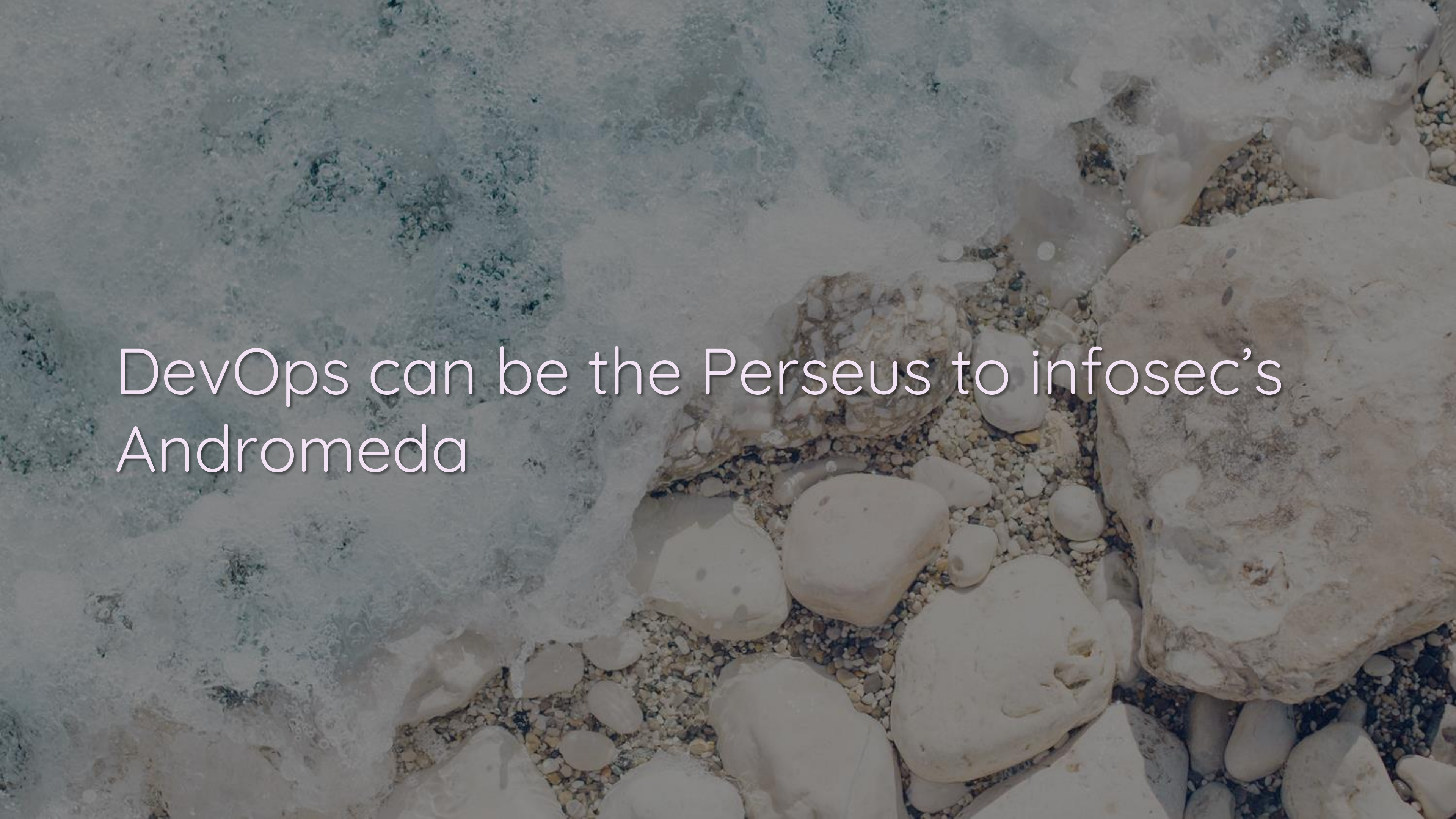
Conclusion

Letting go of core, long-held beliefs is difficult for anyone

Most of infosec’s fears of modern tech distill into fears over losing control

Redirect grasping at phantasms towards control of meaningful threat mitigation

Work together to codify standards so infosec can focus on securing “pets”



DevOps can be the Perseus to infosec’s Andromeda

Unchain infosec from their fears & bring forth a new dawn of secure & resilient software delivery performance

@swagitda_

/in/kellyshortridge

kelly@greywire.net