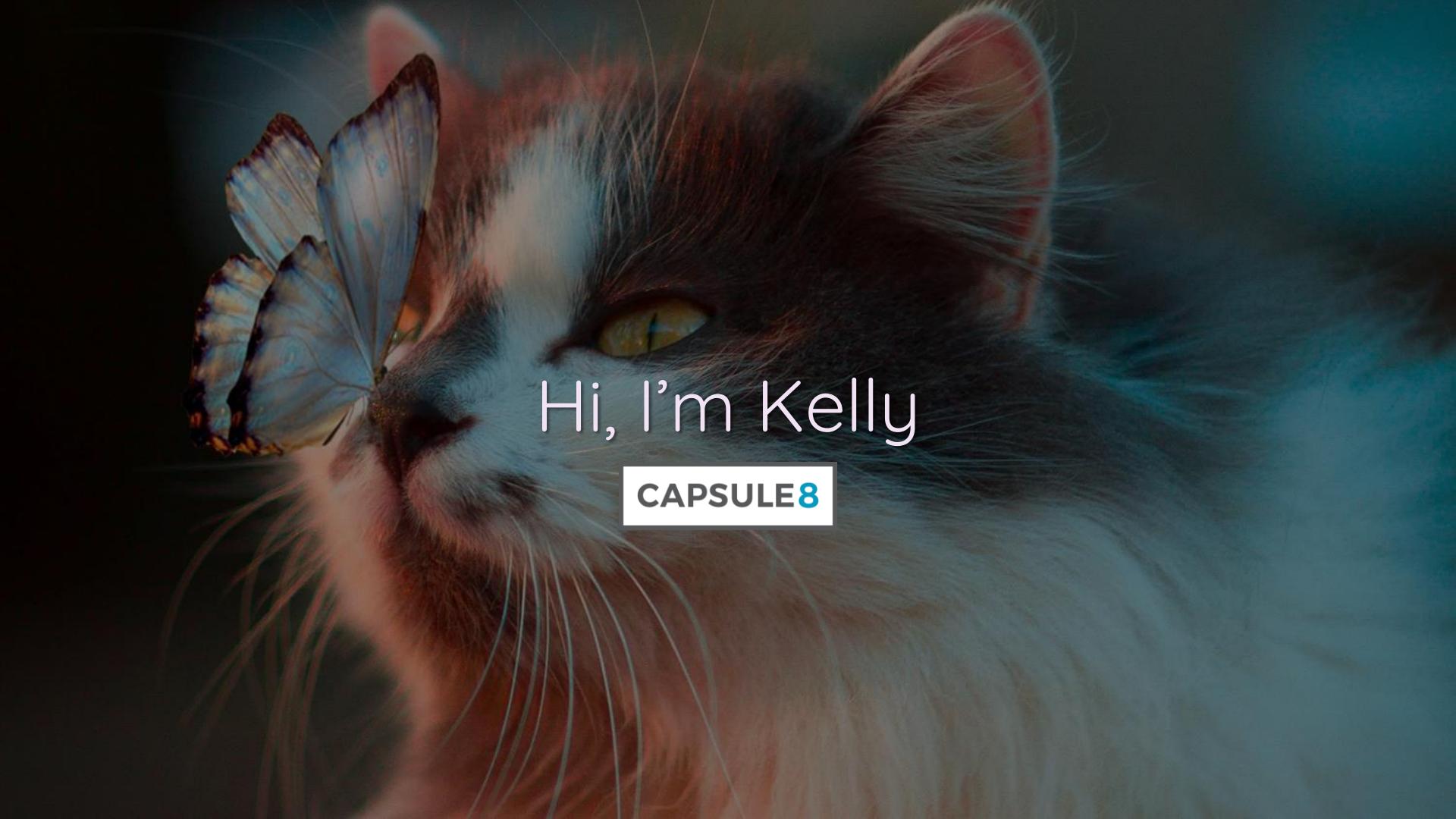




Security Delusions

Kelly Shortridge (@swagitda_)
QCon NYC 2019



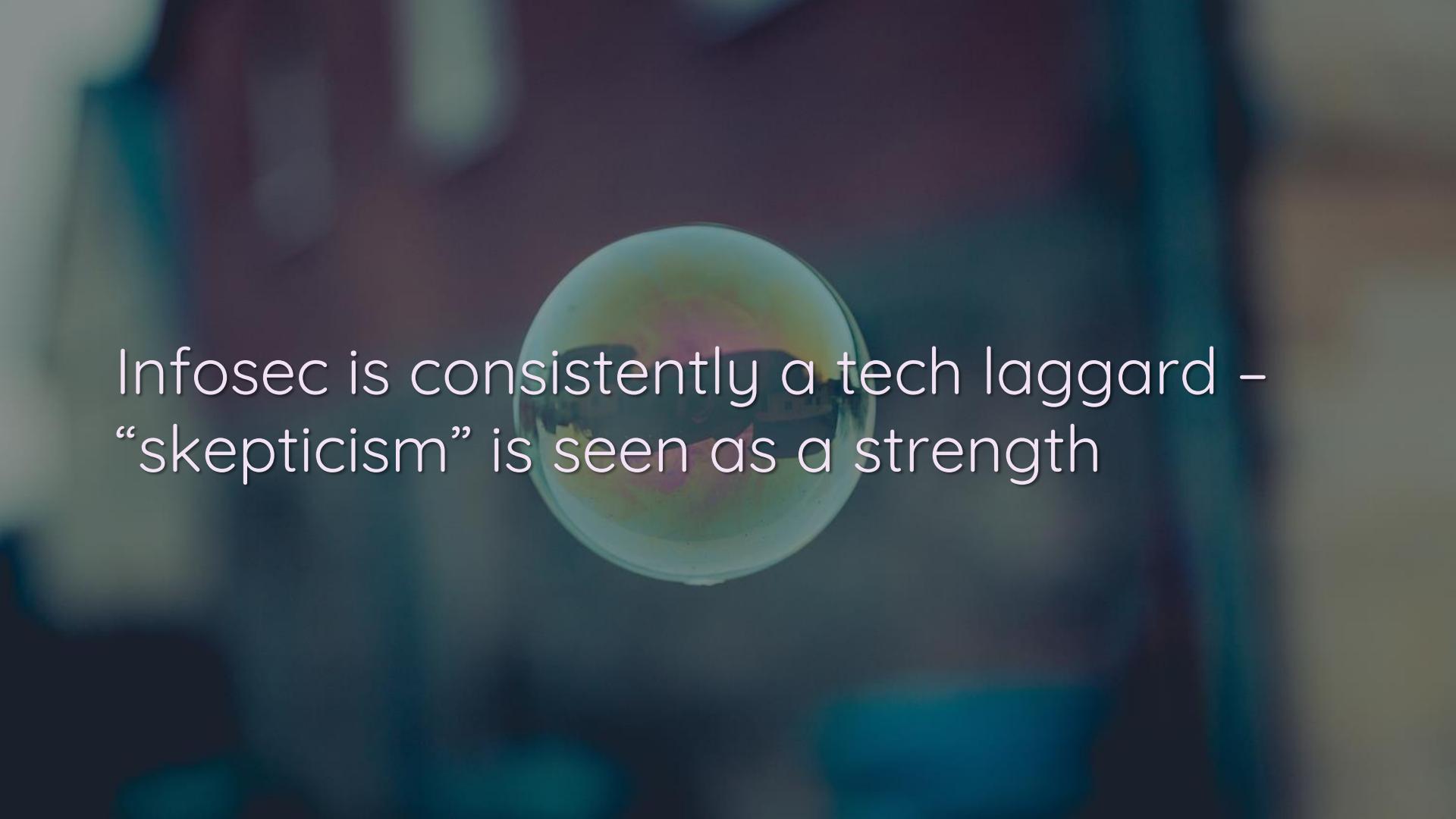
Hi, I'm Kelly

CAPSULE8



“Ignorance is the parent of fear.”

– Herman Melville, *Moby Dick*



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

A wide-angle landscape photograph of a green pasture under a dramatic, cloudy sky. A faint rainbow arches across the upper portion of the image. In the foreground, two sheep stand prominently in the center-right; one is a smaller lamb, and the other is a larger ram with prominent curved horns. Several other sheep are scattered across the field in the background. Distant hills or mountains are visible through the clouds.

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...

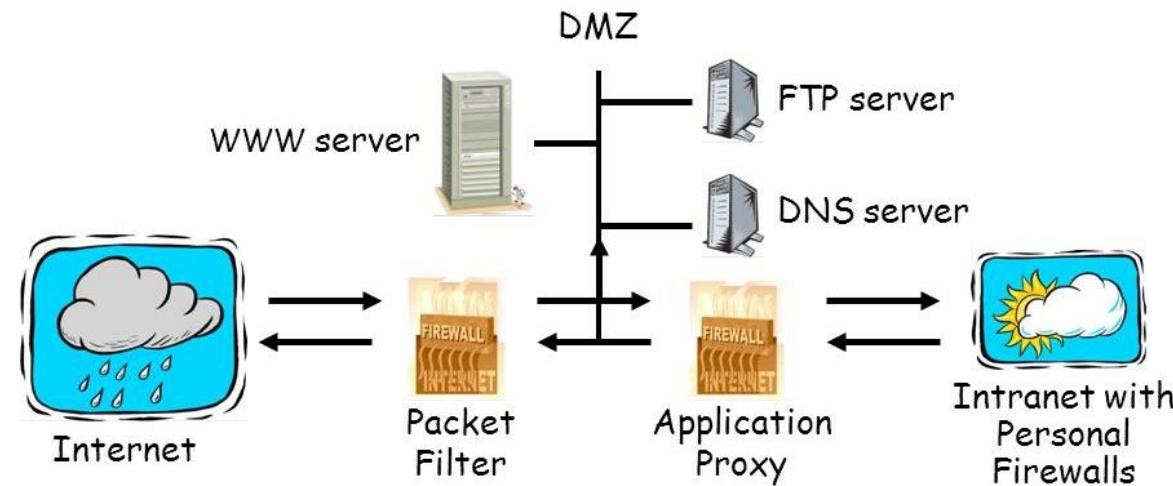


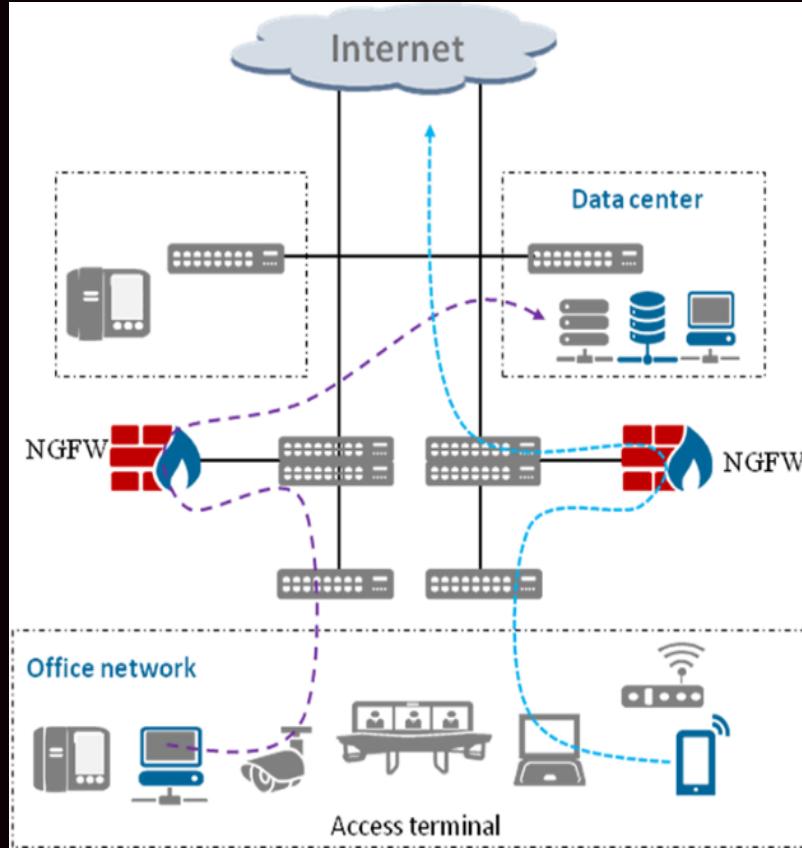
The crux of cloud fear was rooted in a loss of control by the infosec team

The firewall was always the center of the enterprise infosec universe

Firewalls and Defense in Depth

- Example security architecture





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

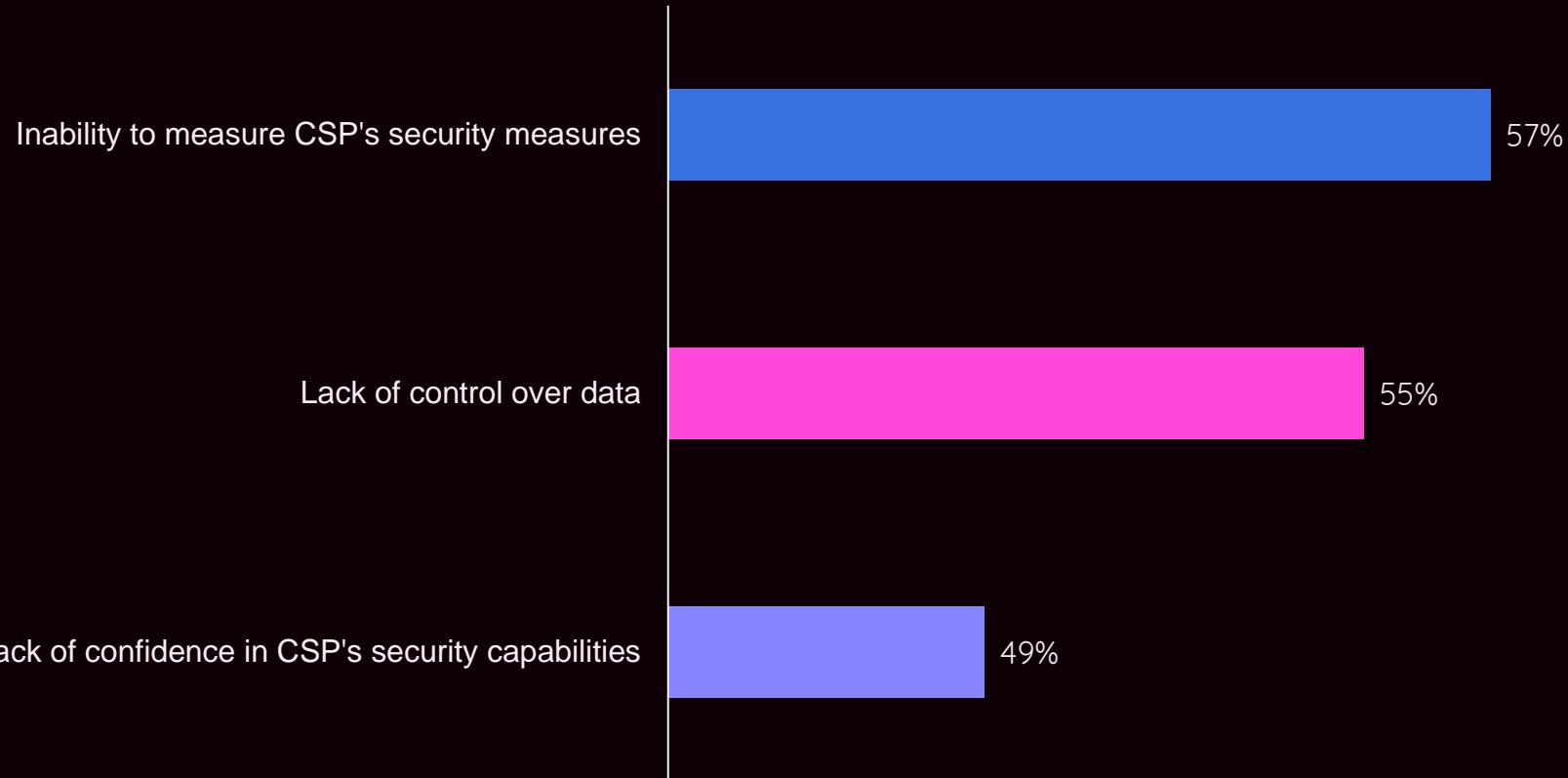


Cloud + microservices represents a
Copernican revolution for infosec

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



2012: “What is holding back cloud?”

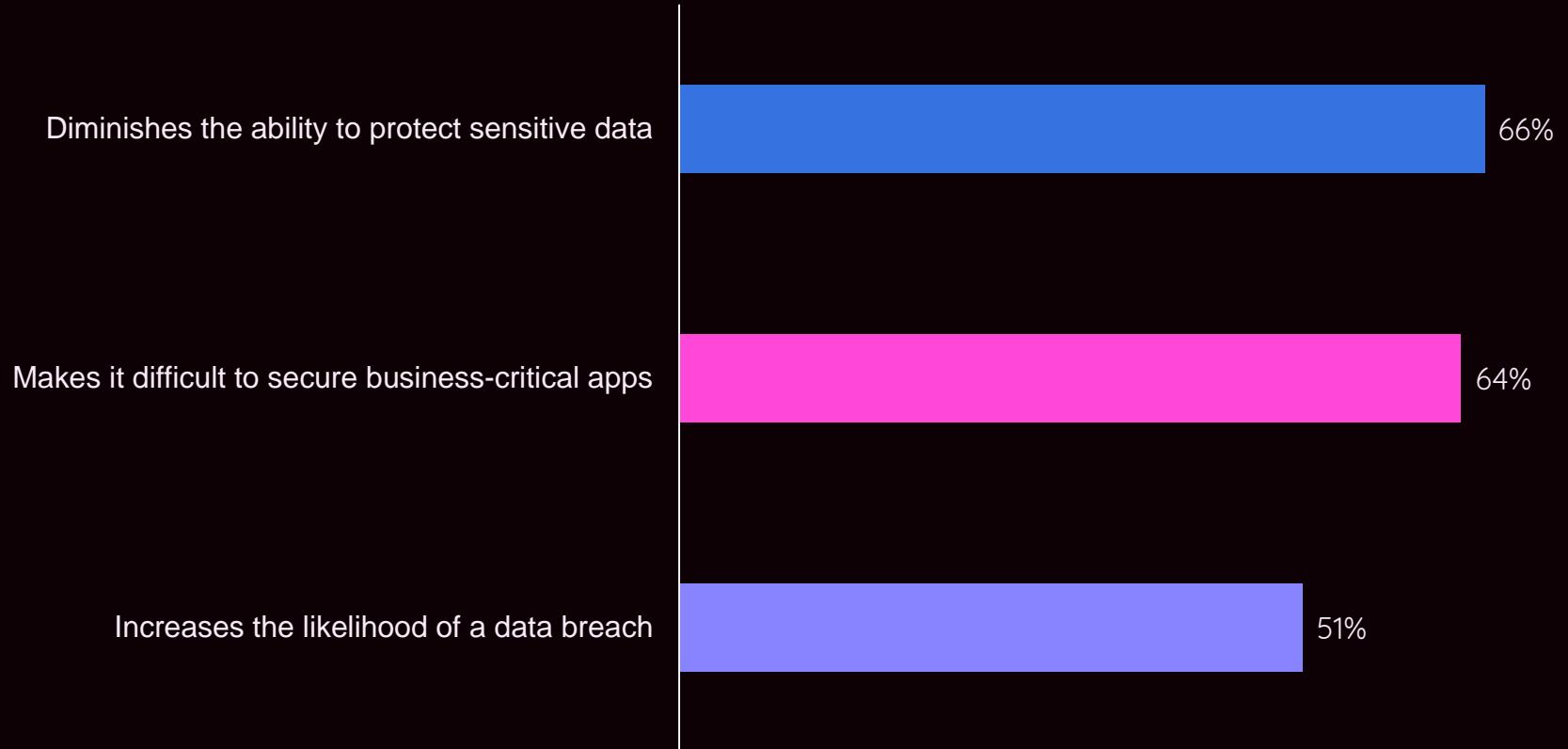


Source: Intel

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



2014: Cloud Multiplier effect on security

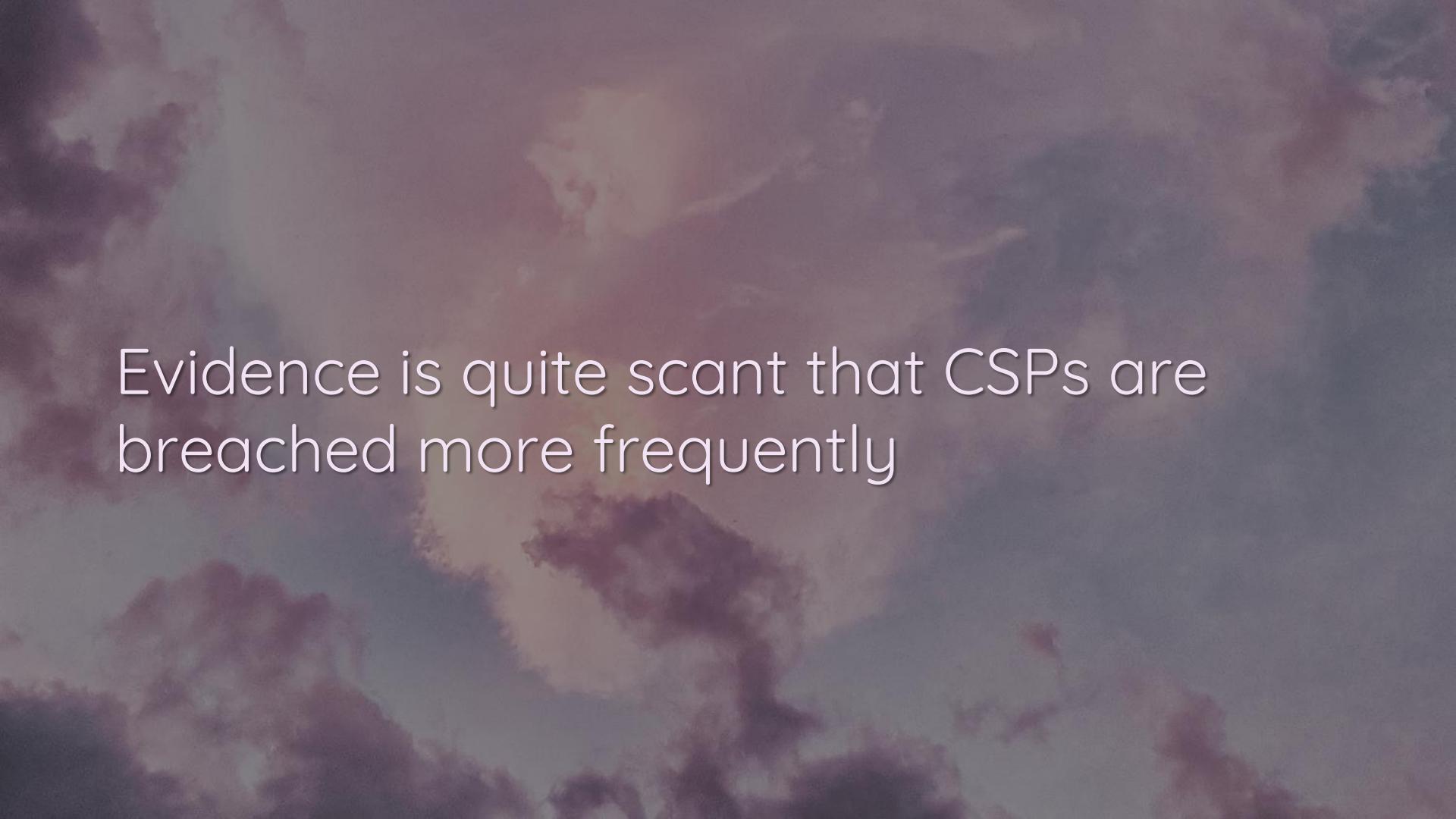


Source: Ponemon

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

A yellow rubber duck is floating in water, surrounded by colorful bubbles. The background is a blurred gradient of blue and green.

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 \times 10,000 =
infosec's mental model of microservices

A dark, atmospheric photograph of a Swiss castle at dusk or night. The castle, with its multiple towers and spires, is illuminated from within, casting a warm glow against the cool blues and purples of the twilight sky. A stone bridge leads from the foreground towards the castle. In the background, a range of snow-capped mountains is visible across a body of water, their peaks catching the last light of the day.

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

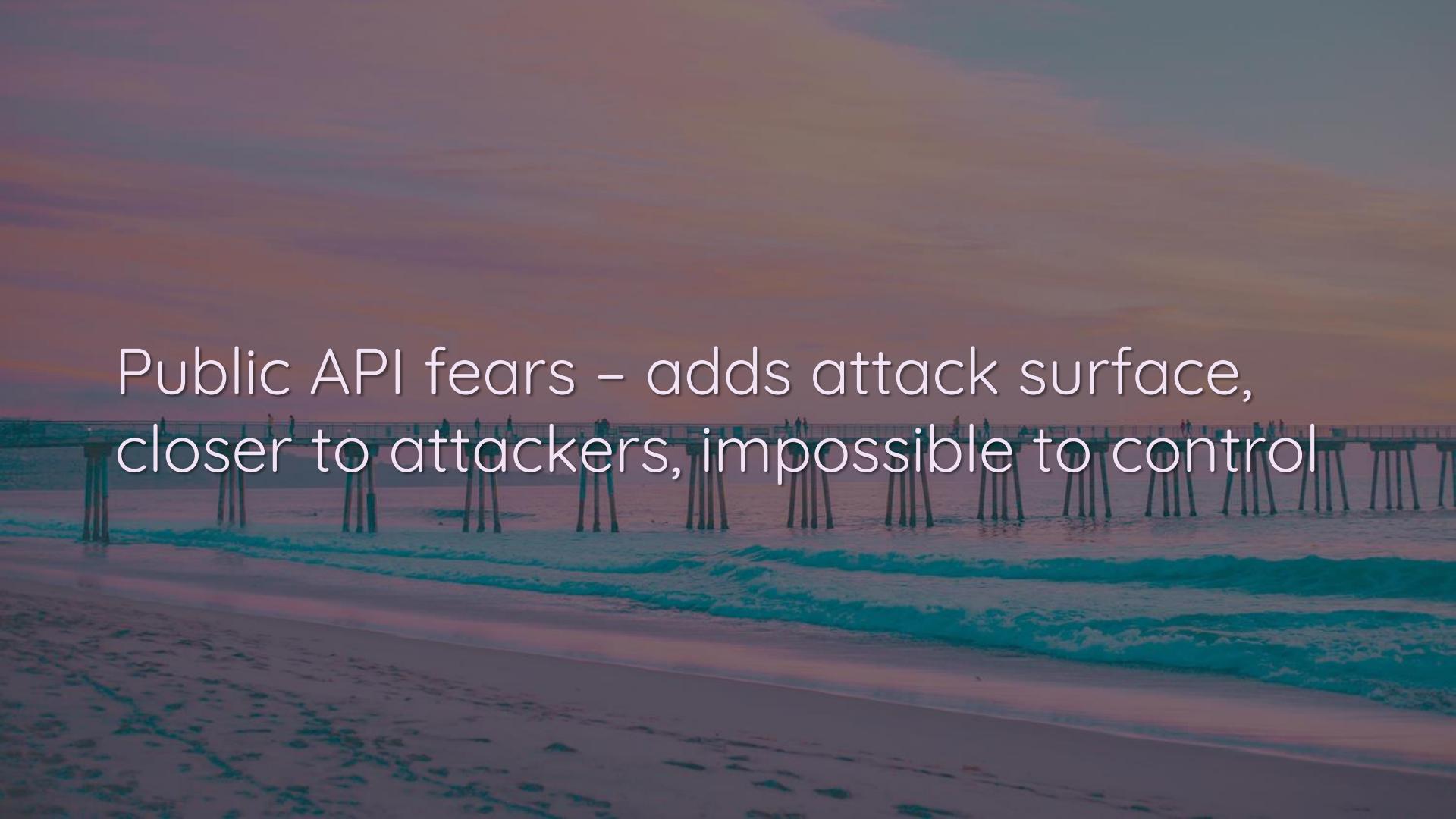
Real history: lateral movement was easy
because everything else was #yolosec

A photograph of a small, weathered wooden beach hut with a gabled roof and a single window, perched on stilts over a body of water. The hut is surrounded by a metal railing. The background shows a hazy sky and distant land or other structures.

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

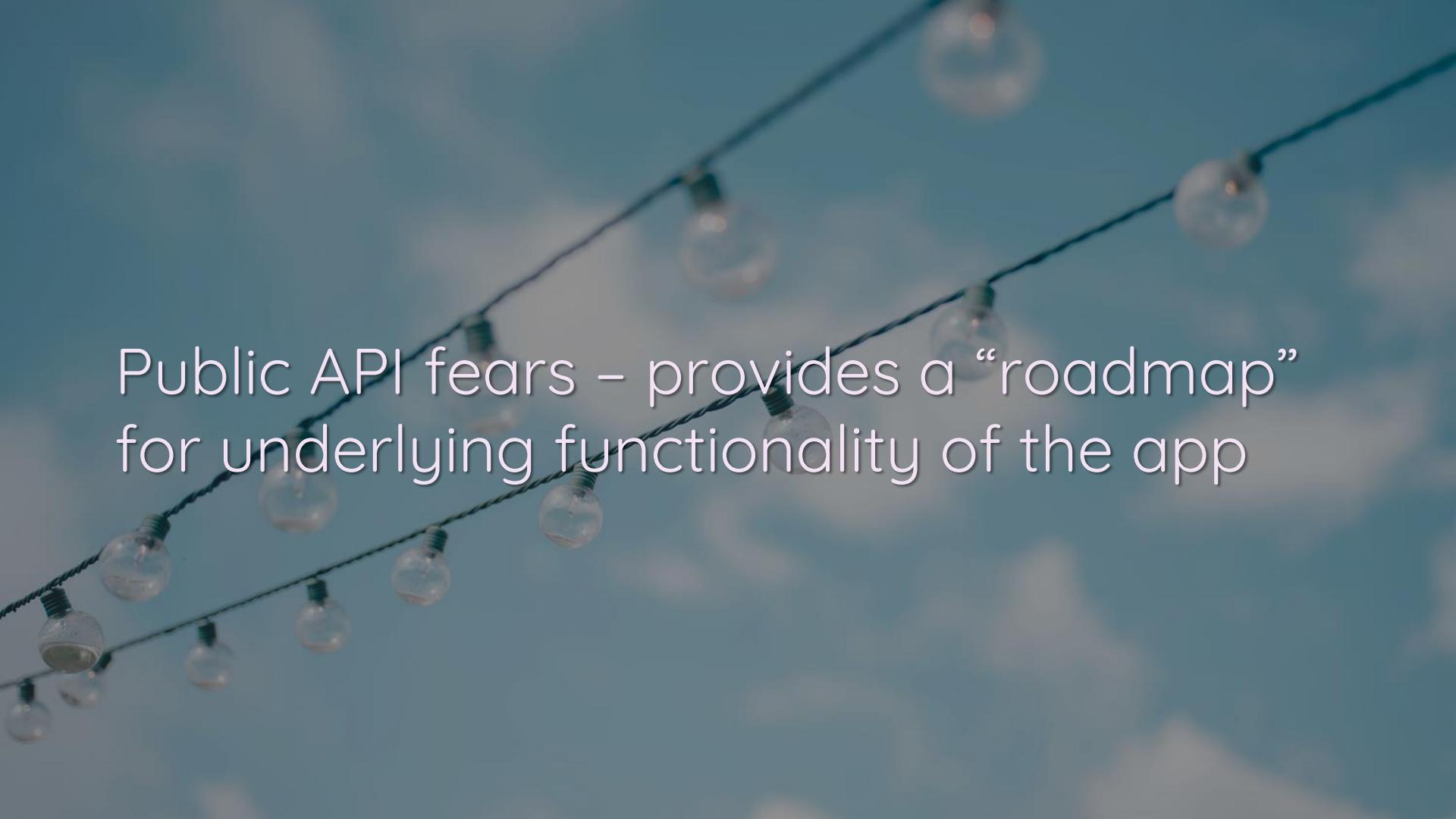
2018: 51% aren't certain the infosec team
knows all APIs within the organization

Source: Ping Identity

A photograph of a beach at sunset or sunrise. The sky is filled with warm, orange and yellow hues. In the middle ground, a long wooden pier extends from the left side of the frame towards the right, its dark silhouette contrasting with the bright water. The ocean waves are visible, crashing onto the sandy shore. The overall atmosphere is peaceful and scenic.

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.”

A decorative string of clear glass lightbulbs hangs across a blue sky filled with wispy white clouds. The lightbulbs are illuminated from within, casting a warm glow. They are suspended by thin black wires against a backdrop of a clear, slightly hazy blue sky.

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

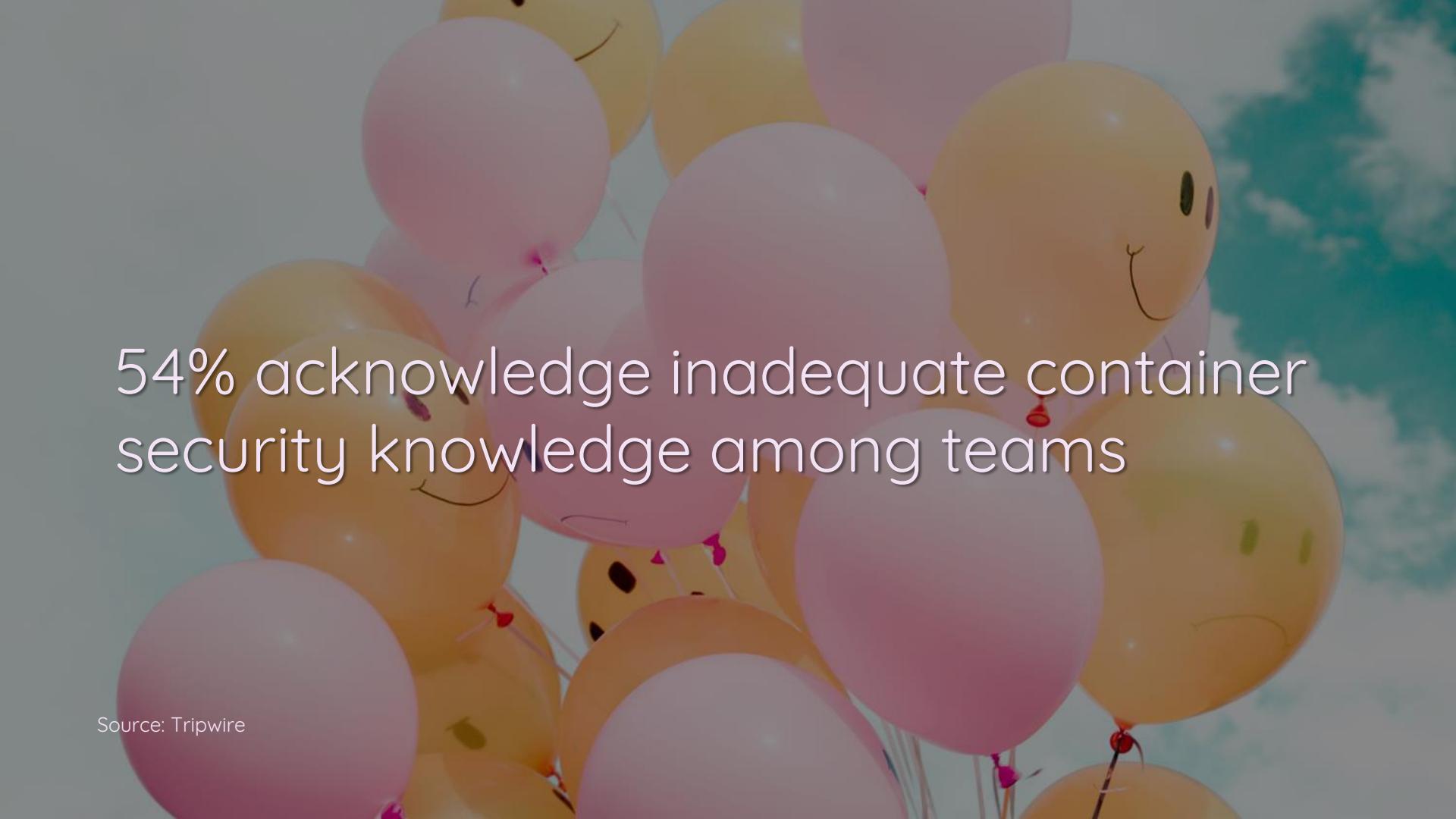




Few in infosec realize containers aren't
just featherweight VMs

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

Source: Tripwire

A cluster of colorful balloons with faces, set against a background of a blue sky with white clouds.

54% acknowledge inadequate container security knowledge among teams

Source: Tripwire

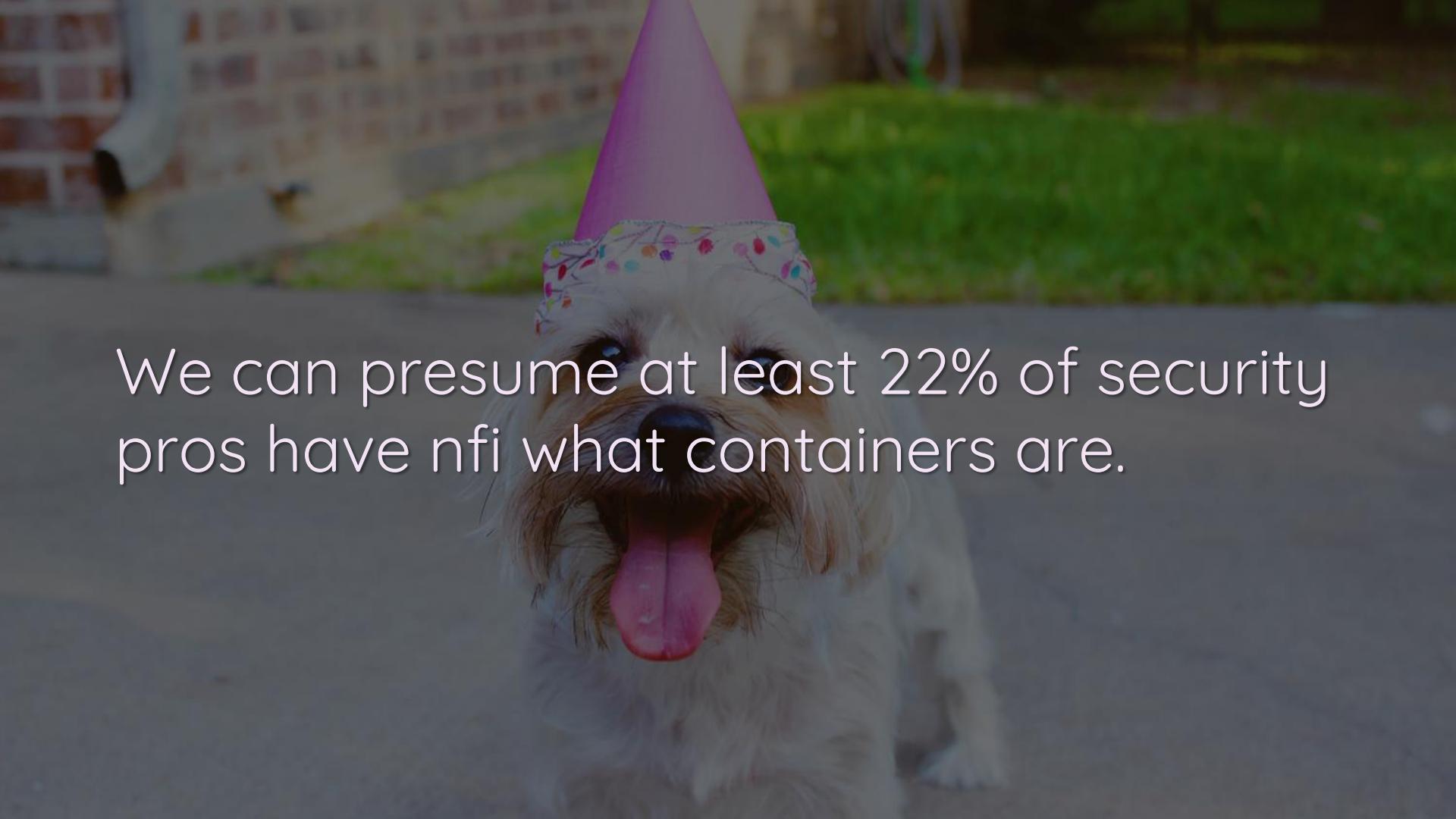


Source: Tripwire

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

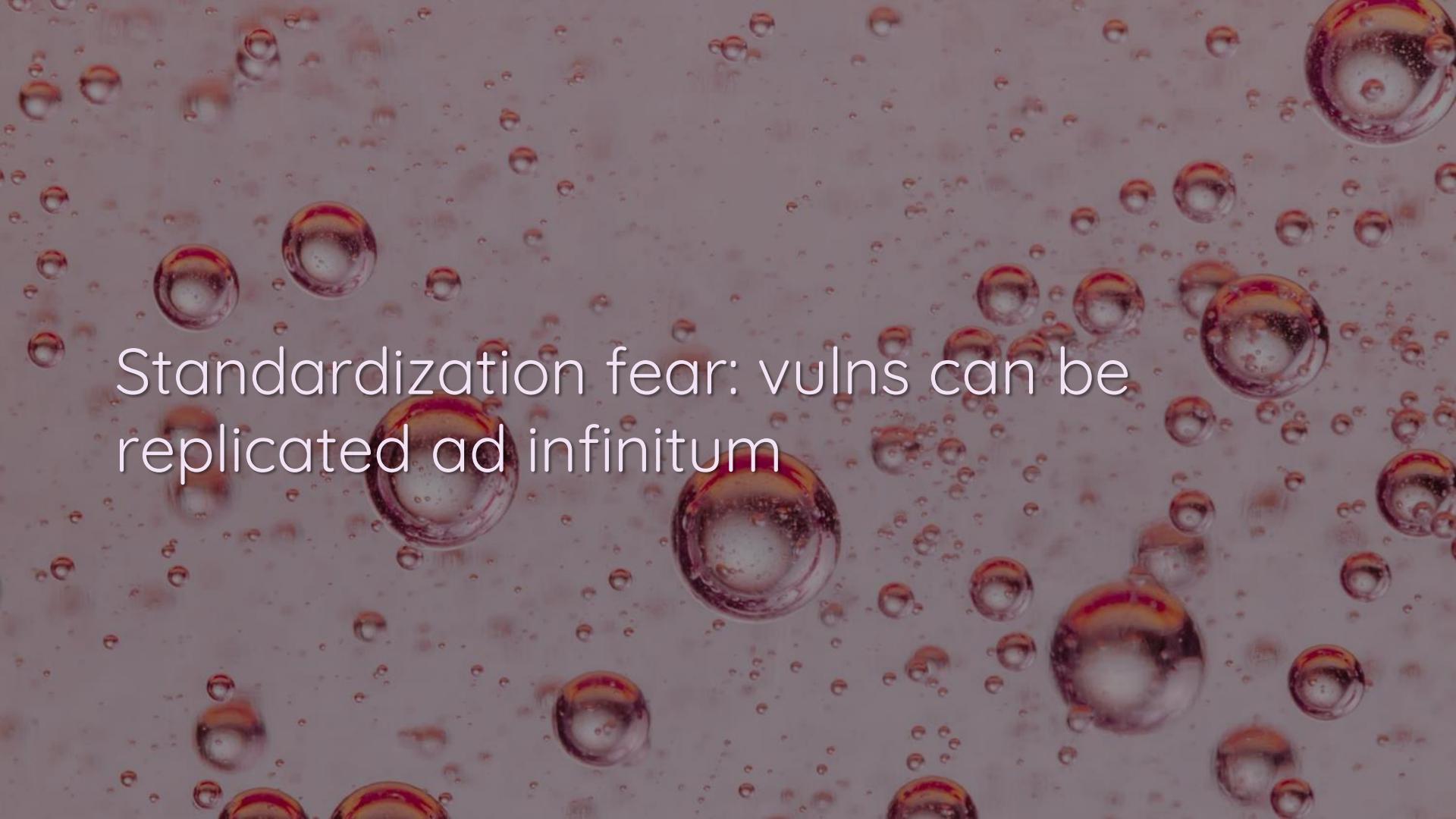
40% want “AI security analytics” & 22% want “blockchain” to secure containers.

Source: Tripwire

A close-up photograph of a small, white, shaggy-haired dog, possibly a Yorkie or Lhasa Apso mix. The dog is wearing a pink party hat with a decorative band featuring small, colorful dots. Its tongue is playfully sticking out. The background is blurred, showing a brick wall and some greenery.

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

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

A background image of numerous small, clear water droplets scattered across a light gray surface. Some larger, more prominent droplets are visible, reflecting light and showing slight color variations. The overall texture is slightly grainy.

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”

A stack of six light green macarons with a dark green filling is positioned on the left side of the frame. To the right of the macarons is a clear glass bottle containing a white liquid, likely milk, with a pink and white striped straw visible.

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.?

A photograph of a person's hand holding a single, light-colored scallop shell. The shell has a distinct radial pattern of ridges. The hand is positioned in the lower-left foreground, with the shell held between the thumb and forefinger. The background is a blurred landscape of a sandy beach meeting a calm sea under a clear blue sky.

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?

A photograph of a person's hand holding a lit sparkler above the water. The hand is positioned vertically, with the sparkler pointing upwards. The water is dark and reflects the light from the sparkler. In the background, there are small, scattered lights or confetti-like particles floating in the air, suggesting a festive or celebratory atmosphere. The overall mood is mysterious and intimate.

Cheat Codes for Dealing with
This Mess

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

A dark, moody photograph of a man wearing a mask. The mask has "KISS ME" written across the forehead in red spray paint. He is holding a can of spray paint in his hand. The background is dark and hazy.

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.”

A background image showing several colorful smoothies or milkshakes in different glasses and containers, topped with various toppings like sprinkles and fruit. The colors are vibrant and varied.

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

A photograph of two glowing incandescent lightbulbs against a dark background. One bulb is in sharp focus in the foreground, while another is slightly blurred in the background to the left.

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

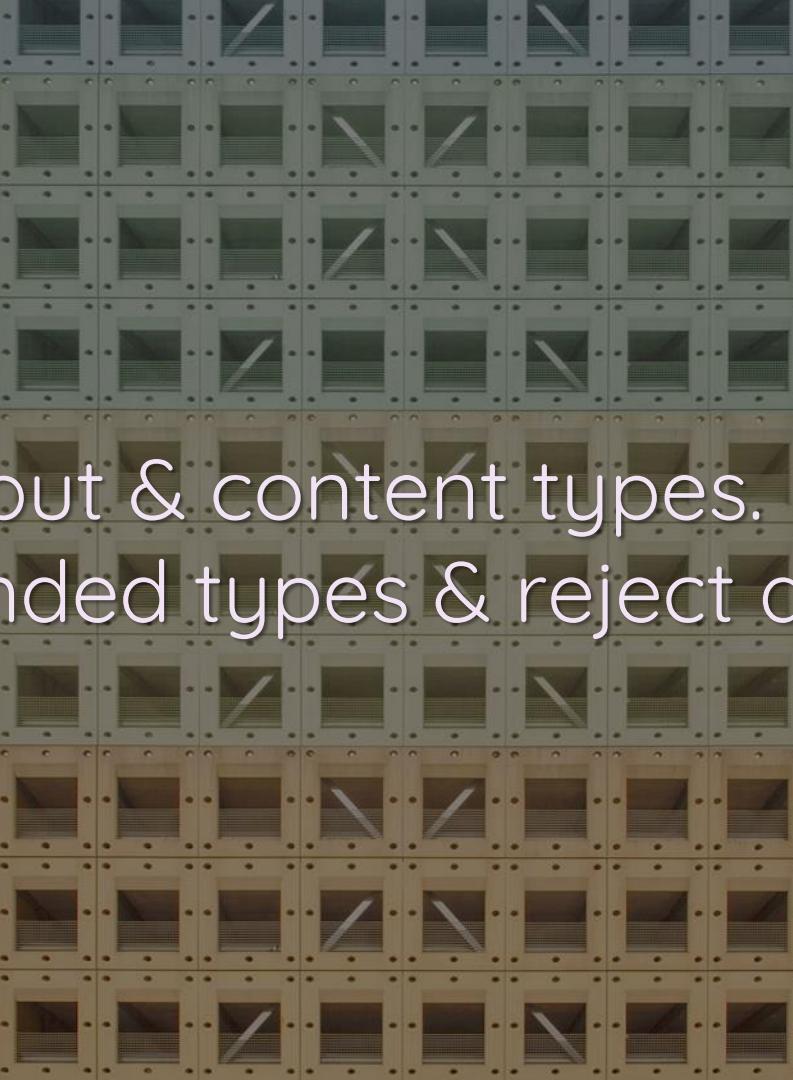
Amazon Inspector + AWS Trusted Advisor are great tools to start

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



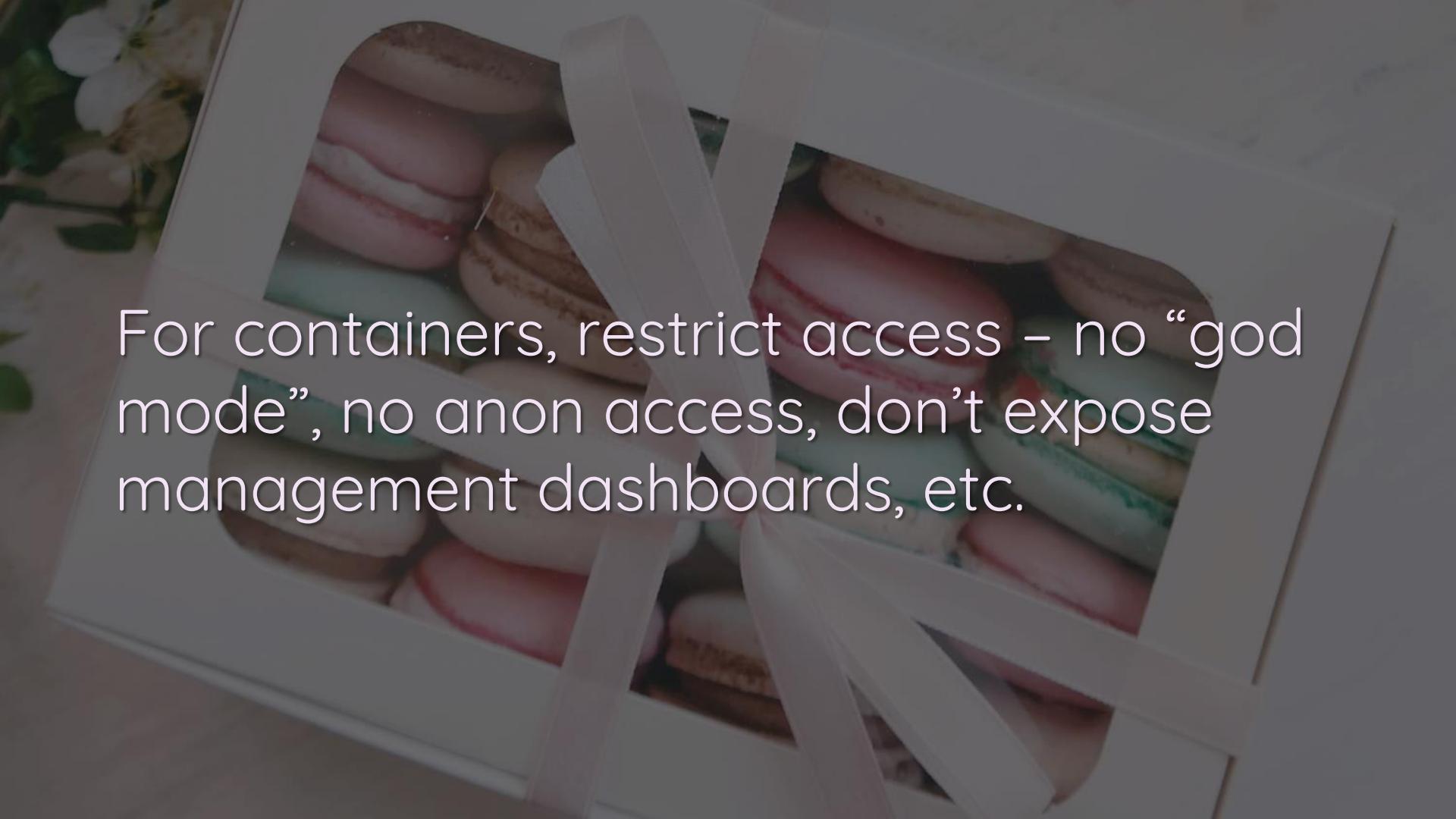
Basic API hygiene will suffice - auth,
validation, & not trusting external data

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

A large, rectangular metal grid structure, possibly a window or a screen, composed of numerous small squares. Each square contains either a dark, solid rectangle or a diagonal white line from the bottom-left corner to the top-right corner. The grid is set against a dark, textured background.

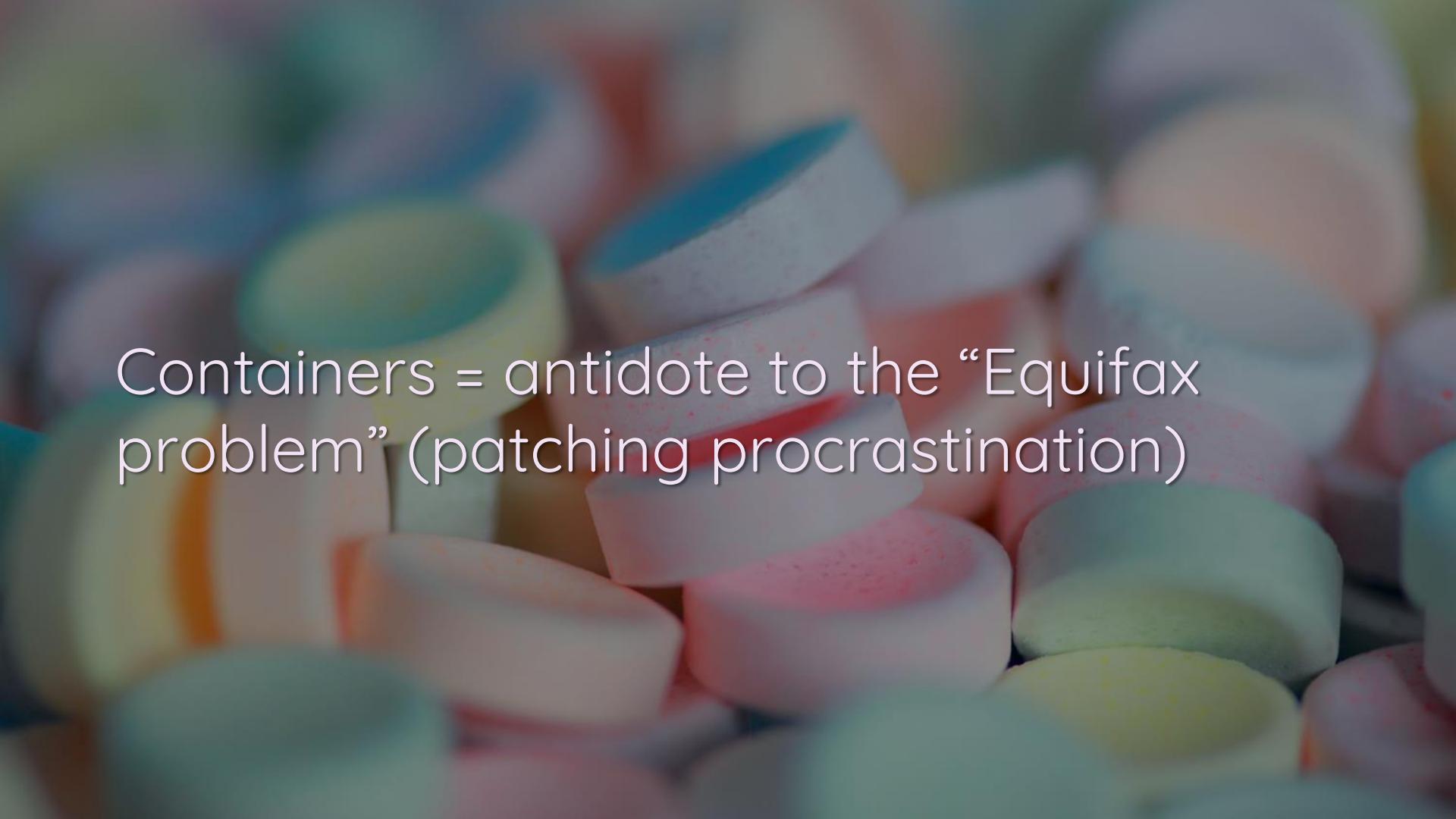
Validate input & content types. Explicitly define intended types & reject all others.

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

A close-up photograph of a white cardboard box filled with colorful macarons. The box is open, showing rows of macarons in various colors like pink, green, and yellow. The top lid of the box is visible, featuring a floral illustration of white flowers and green leaves.

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

A background image featuring a dense, overlapping pattern of numerous small, semi-transparent red and pink circular bubbles of varying sizes, creating a sense of depth and texture.

Live migration means security can patch
without impacting end users

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

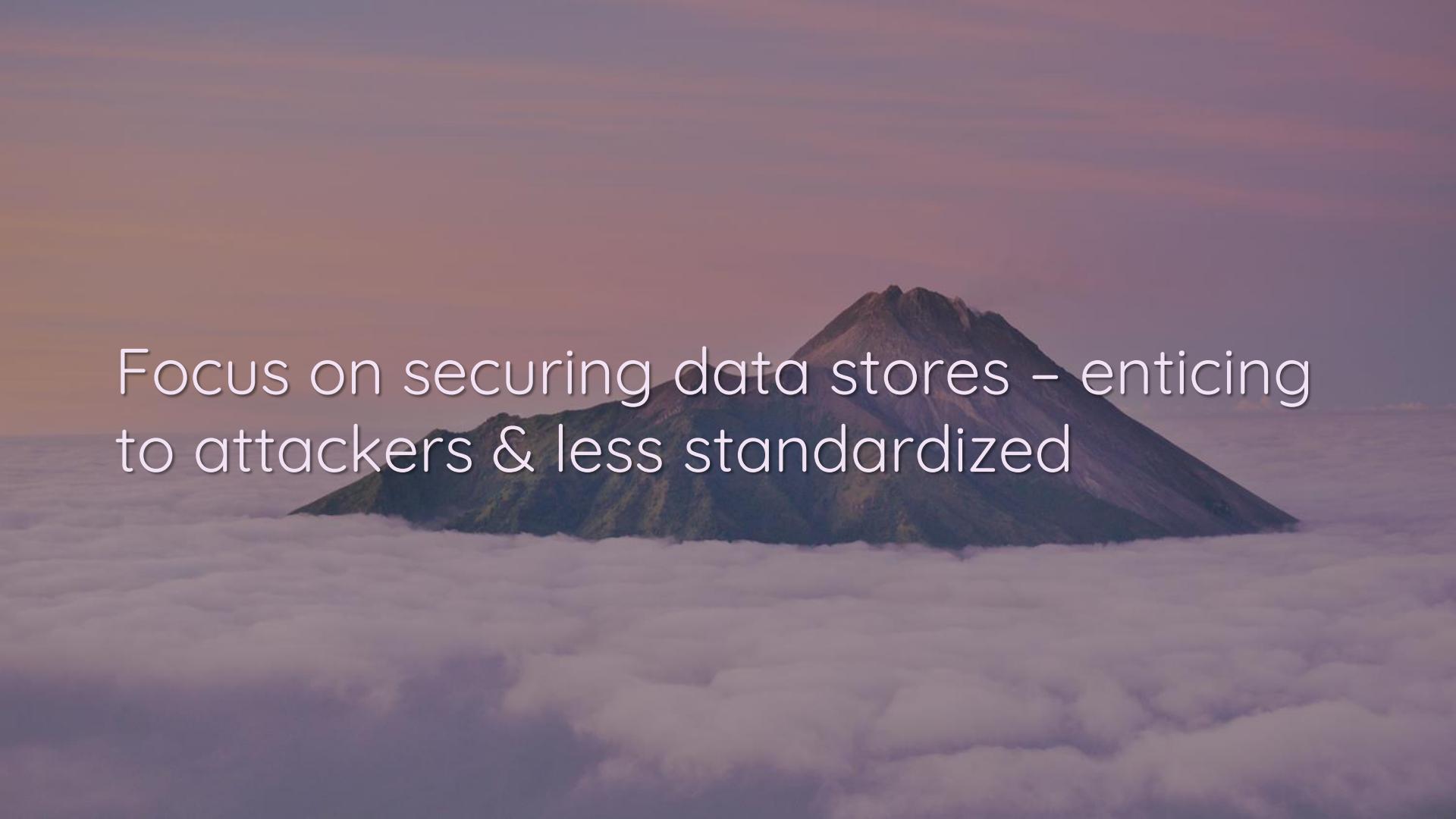


If misconfigs are covered, what remains
for infosec teams to tackle?

The background of the slide features a dark, slightly blurred image of a blue globe on the right and an open book with white pages and a blue cover in the center. The overall atmosphere is professional and academic.

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

A photograph of a majestic mountain peak, likely Mount Fuji, standing tall above a dense layer of white clouds. The sky is a gradient of warm colors, from deep orange near the horizon to a cooler blue-grey at the top. The mountain's slopes are partially covered in snow or dark green vegetation. The overall scene is serene and majestic.

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

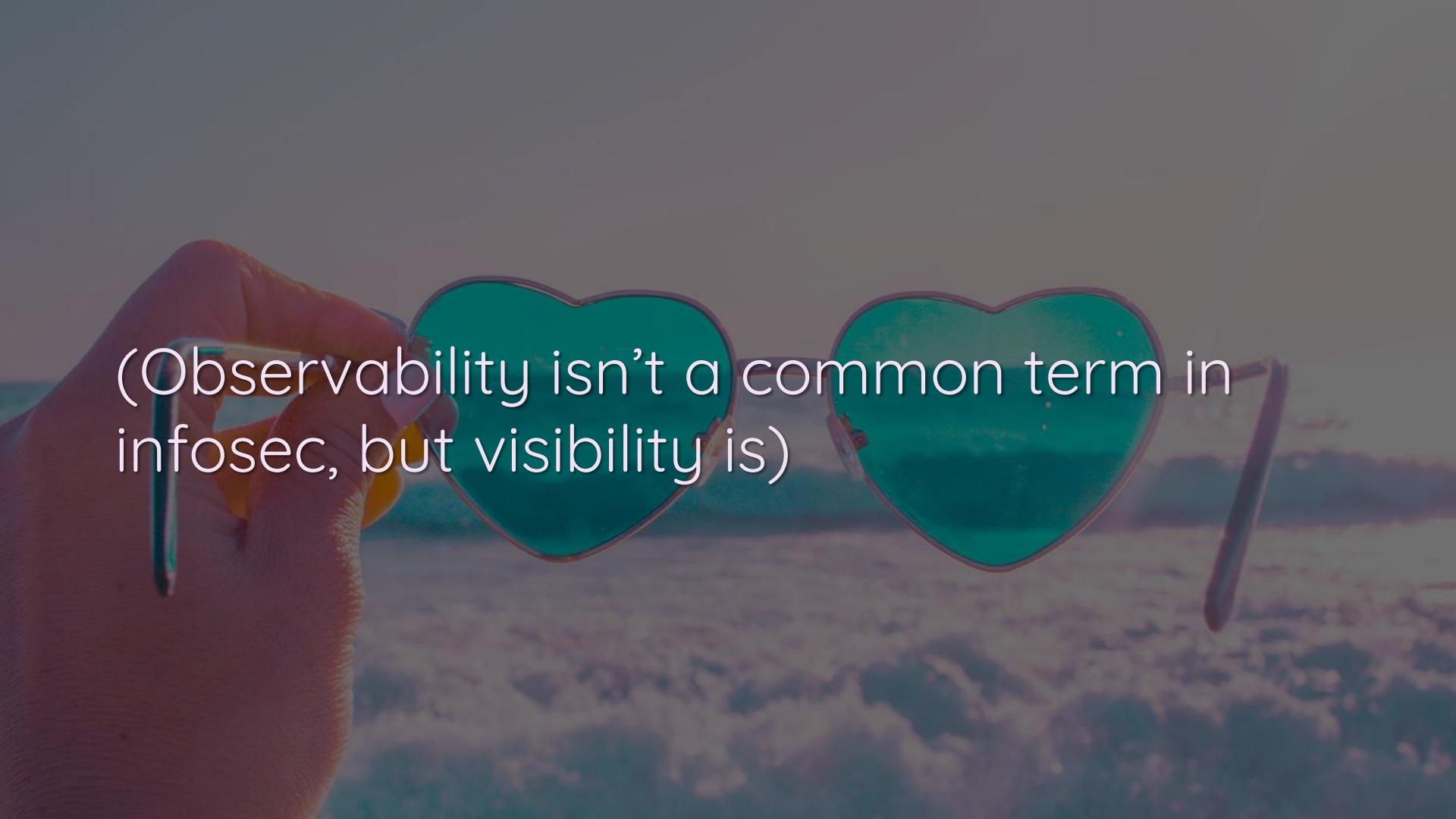
Help infosec finds database visibility & monitoring tools (e.g. Vivid Cortex)

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



Highlight compliance - file integrity monitoring underpins most standards

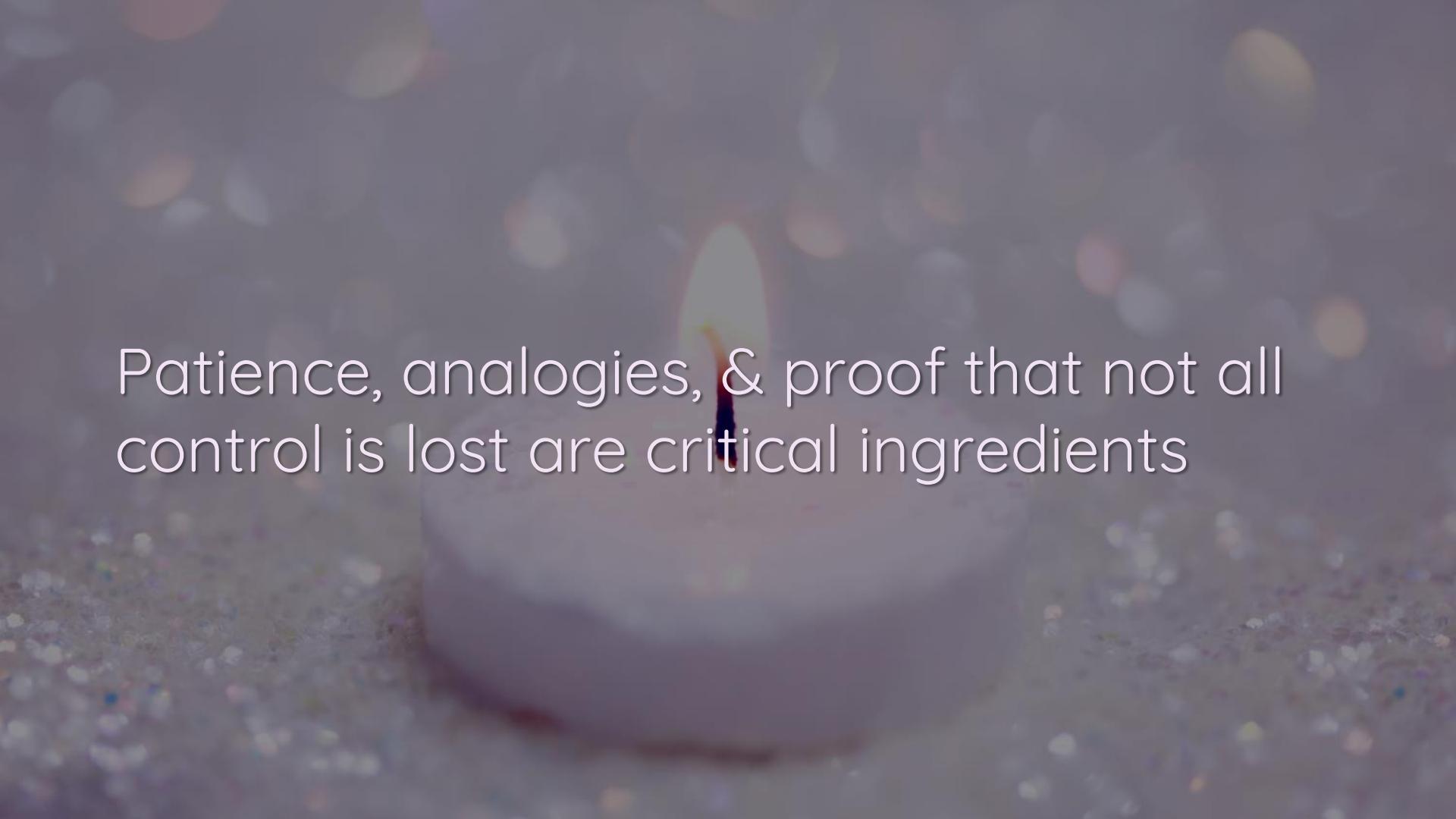
FIM is easier given the improved inspectability of containers

A photograph of a hand holding a pair of heart-shaped sunglasses. The sunglasses have teal lenses and silver frames. They are held up in front of a scenic view of a beach at sunset or sunrise. The sky is filled with warm, orange, and pink hues, and the ocean waves are visible in the foreground.

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

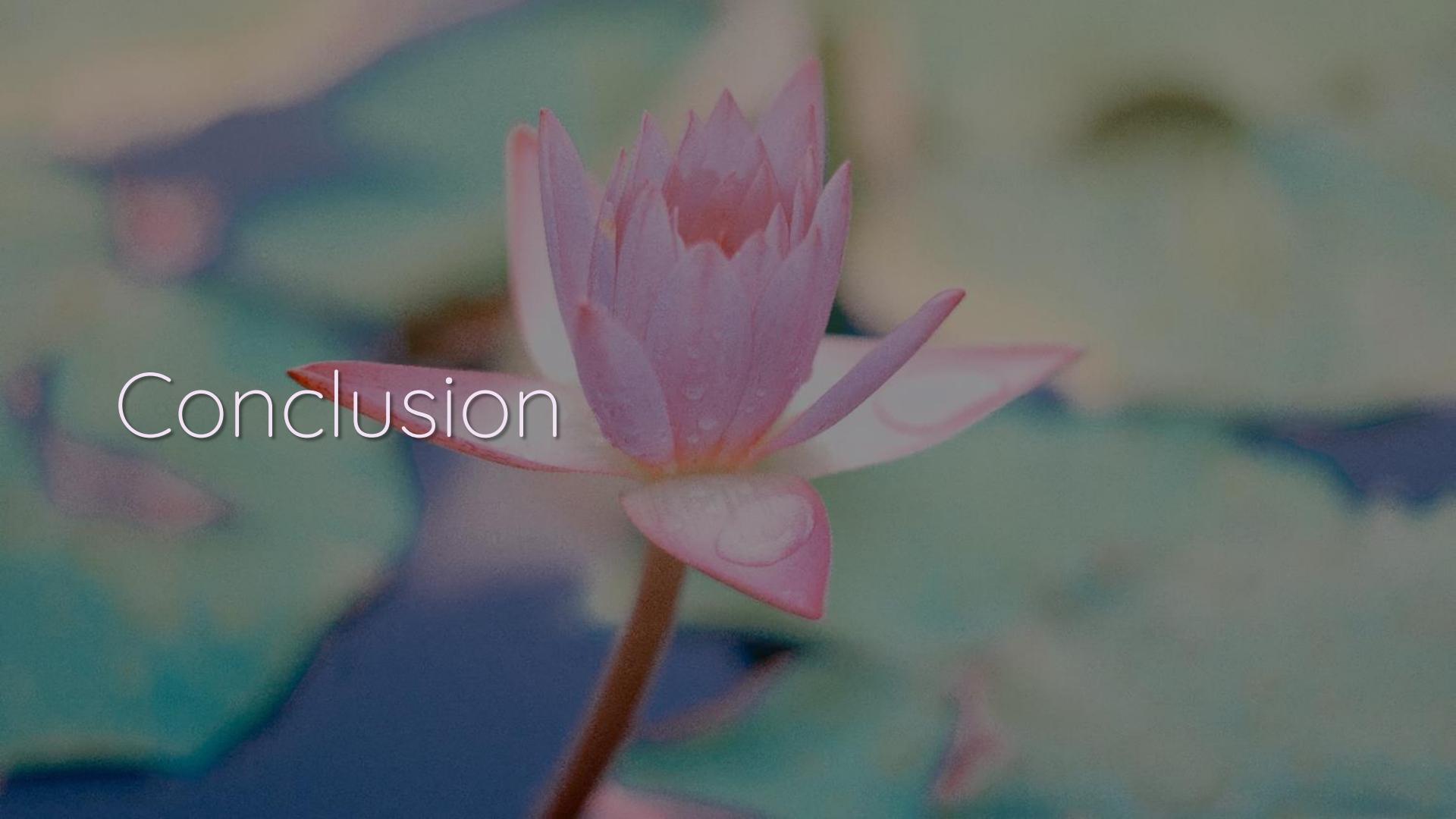
Infosec ppl aren't all the same - different tactics will work to build understanding

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

A close-up photograph of a single lit candle. The candle is white and has a bright, yellow-orange flame at the top. The background is dark and filled with numerous small, out-of-focus colored lights in shades of orange, yellow, green, and blue, creating a bokeh effect.

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

Conclusion





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



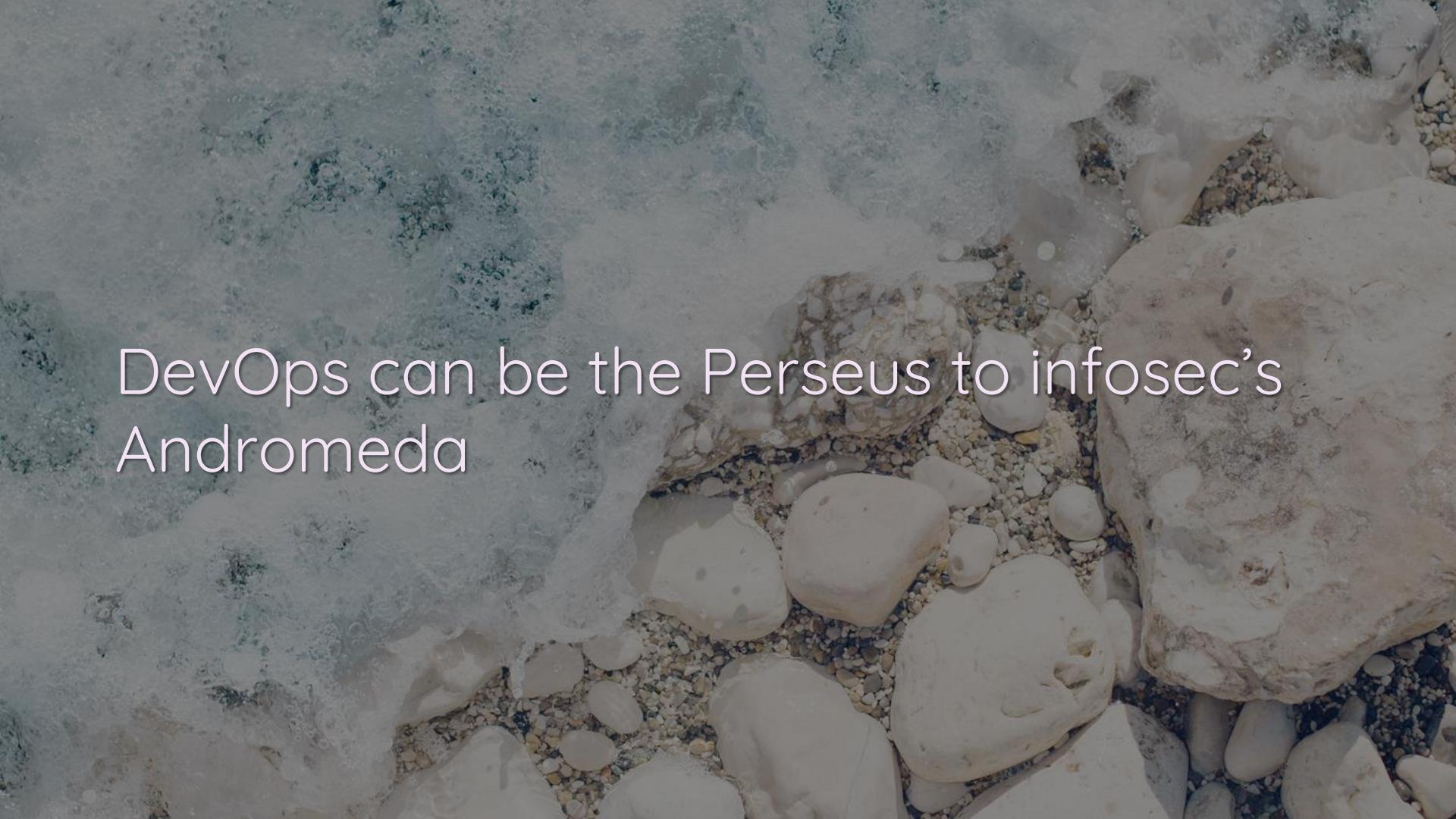
Most of infosec's fears of modern tech
distill into fears over losing control



Redirect grasping at phantasms towards
control of meaningful threat mitigation

A close-up photograph of a fluffy white cat with light blue eyes. The cat is looking directly at the camera with a slightly tilted head. Its mouth is slightly open, showing its tongue and lower teeth. The background is a soft, out-of-focus grey.

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