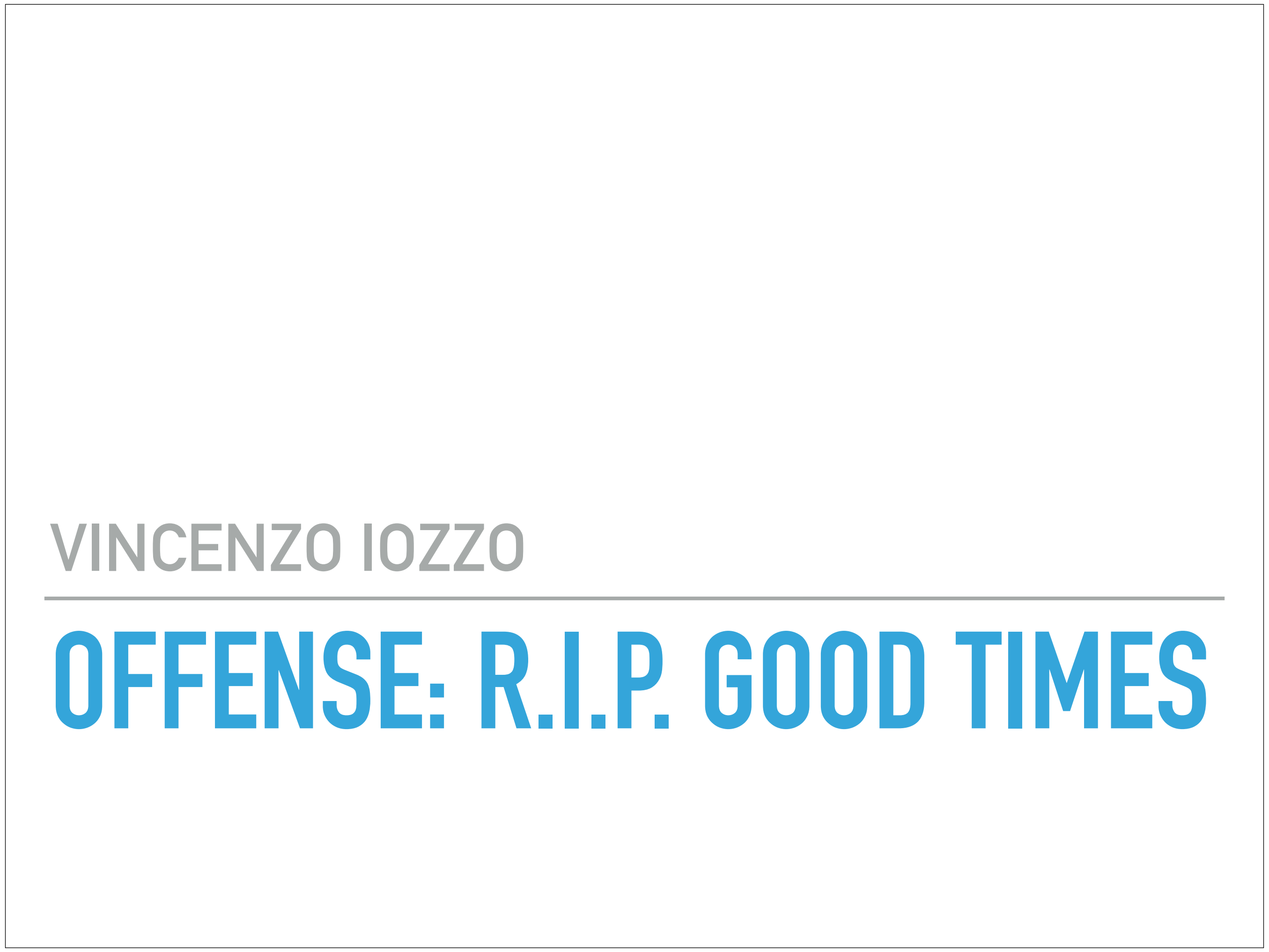
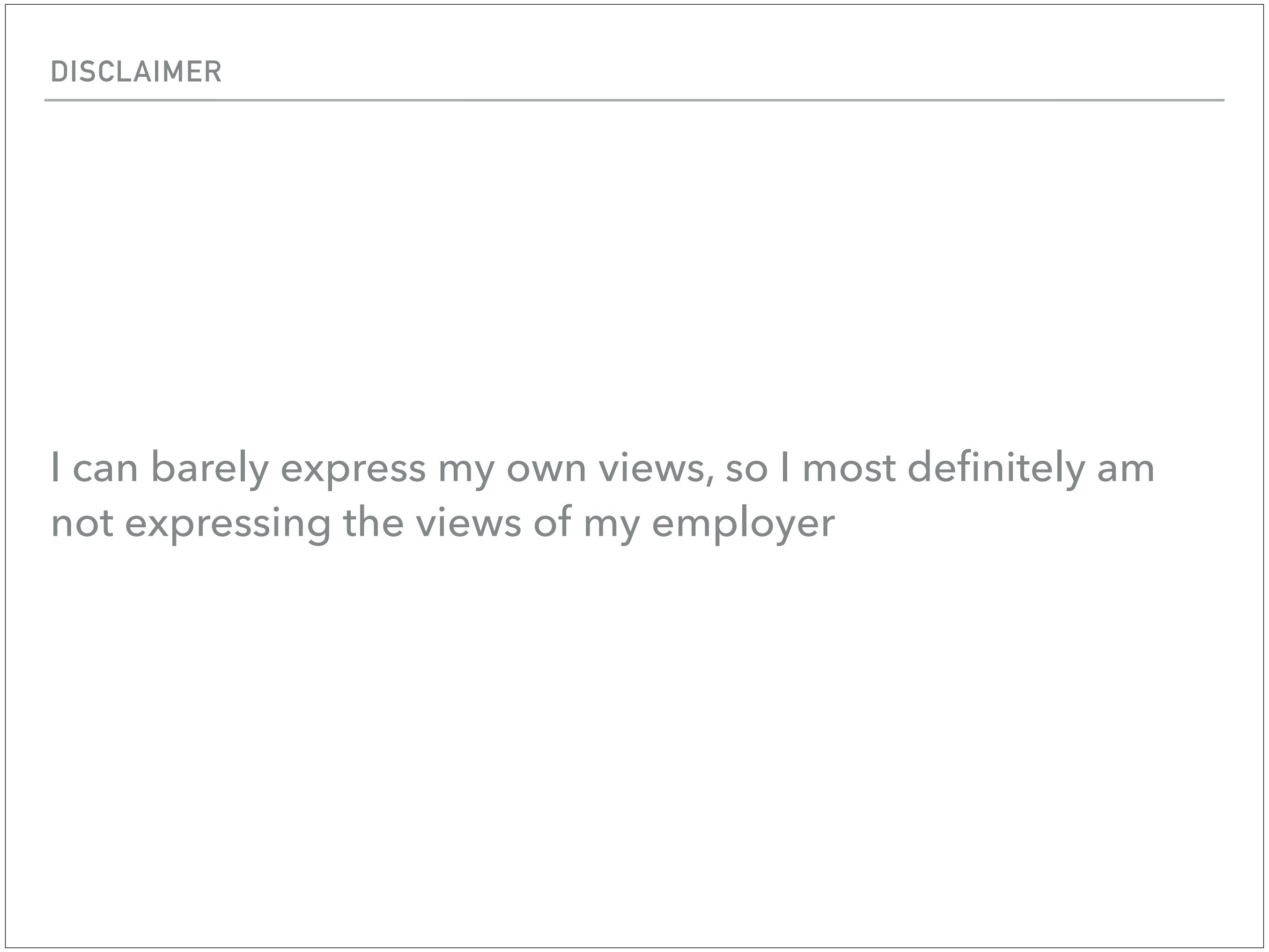


VINCENZO IOZZO

OFFENSE: R.I.P. GOOD TIMES

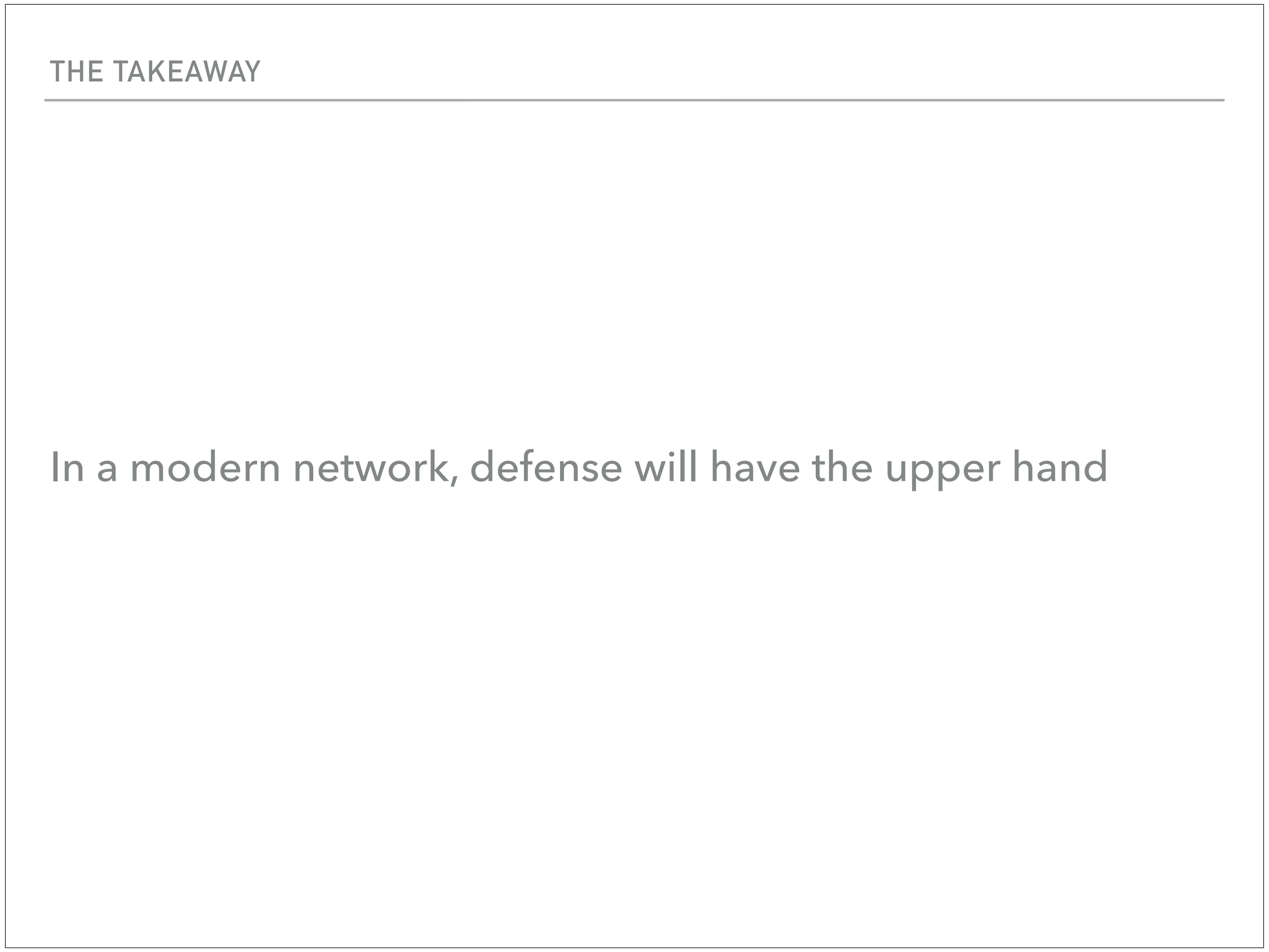
“point and click” data breaches of the kind we are used to will be gone soon or maybe I’m just getting old..



DISCLAIMER

I can barely express my own views, so I most definitely am not expressing the views of my employer

The content and views expressed in this presentation are *not* related in any way to Crowdstrike

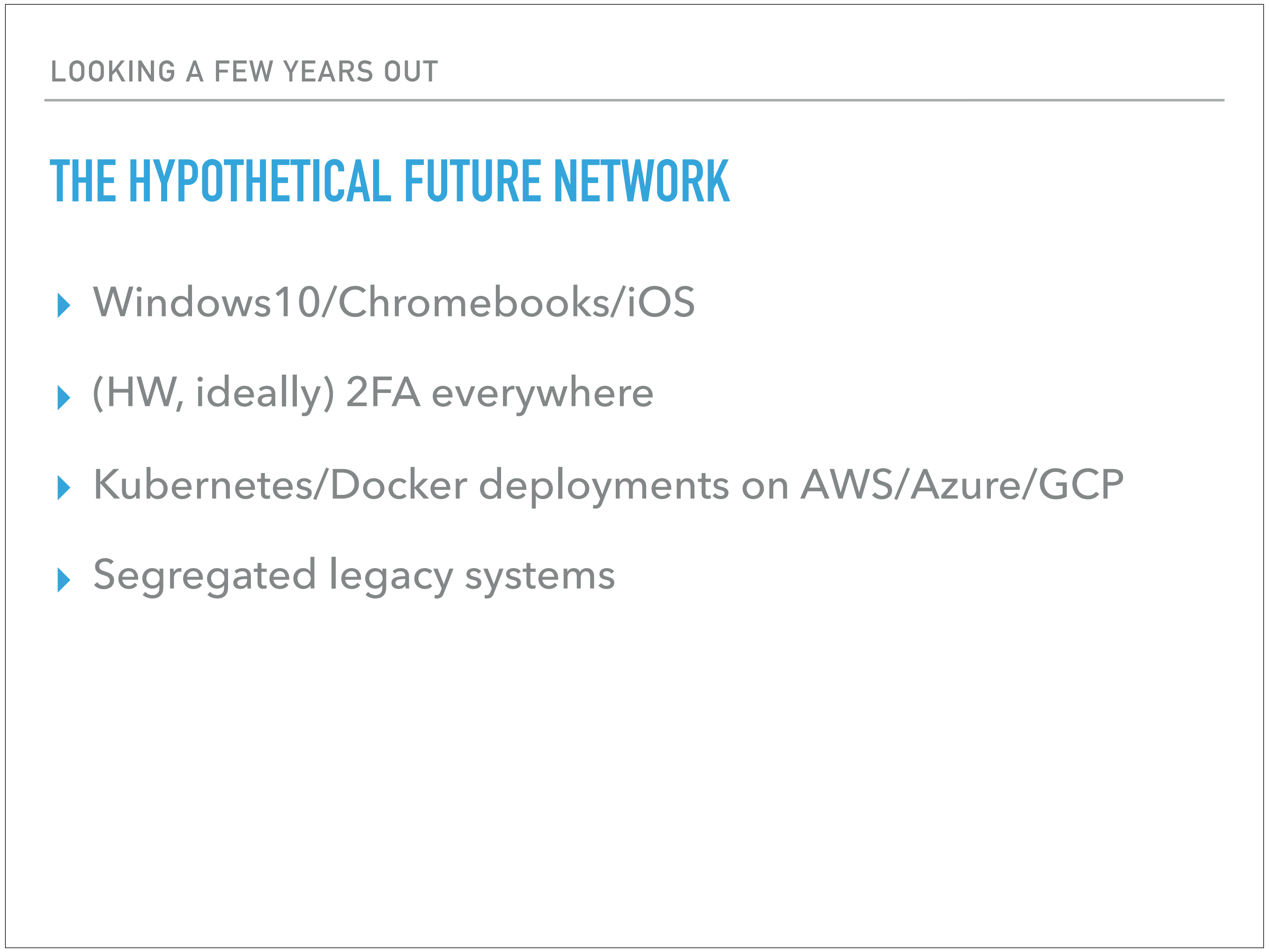


THE TAKEAWAY

In a modern network, defense will have the upper hand

This does not mean that cyber is solved. It just means that attacking a (modern) given system, perimeter or software has more favorable odds on the defense side.

My point is that for the first time we have concrete, stable and usable technology that can make the security posture of a company very hard to compromise at scale.



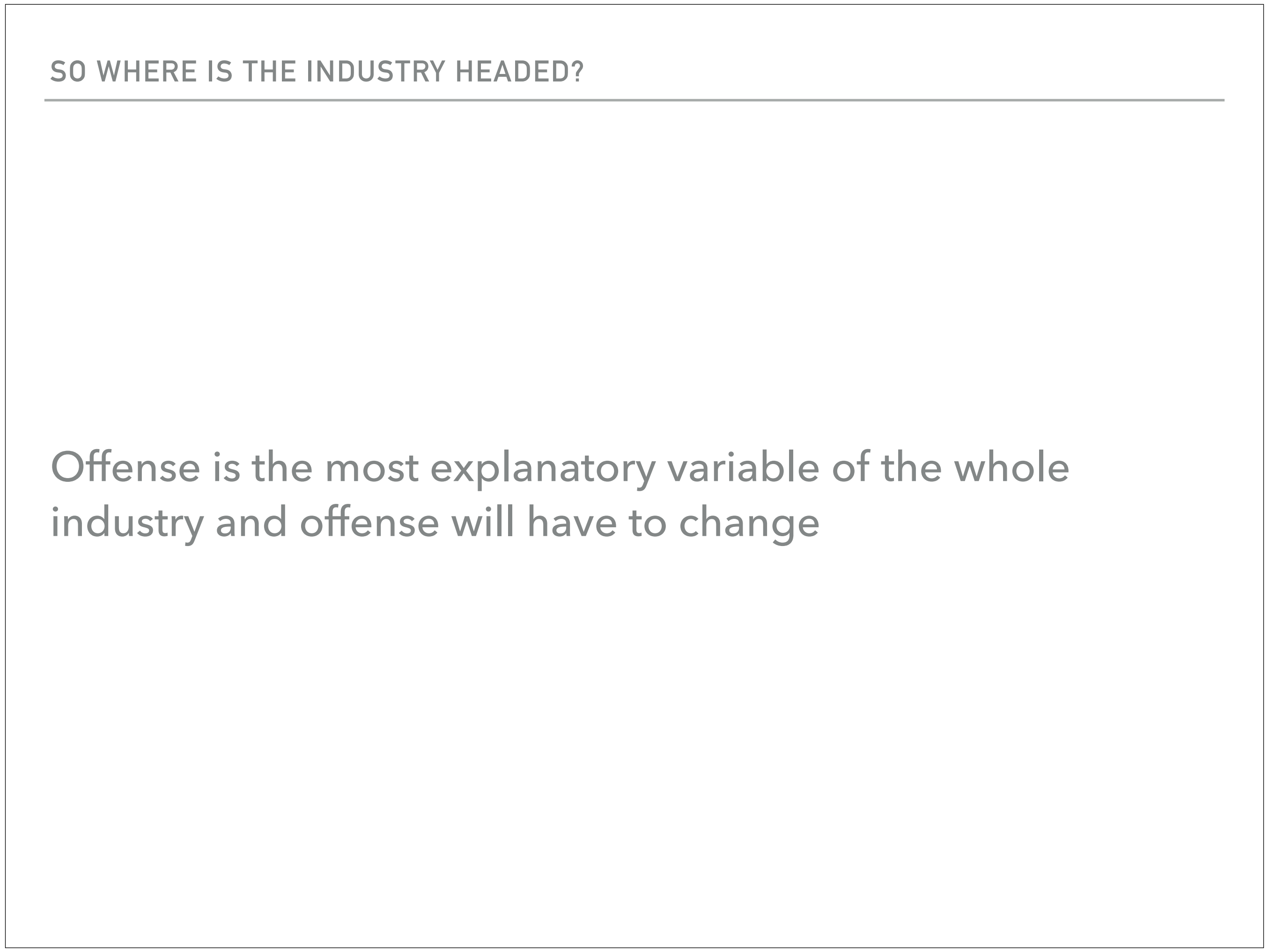
LOOKING A FEW YEARS OUT

THE HYPOTHETICAL FUTURE NETWORK

- Windows10/Chromebooks/iOS
- (HW, ideally) 2FA everywhere
- Kubernetes/Docker deployments on AWS/Azure/GCP
- Segregated legacy systems

Overall adoption of the above is hard to establish but combining a bunch of reports from Gartner and similar the ballpark seems to be 18-20%. Docker adoption growth rate is quite high (about 40% YoY), the rest is harder to establish. The hardest part to estimate is, of course, what “adoption” really means.
Let’s assume that this will be the reality of a network for about 30-40% of the organizations in 5-10 years time.

https://www.gartner.com/smarterwithgartner/6-best-practices-for-creating-a-container-platform-strategy/
https://www.datadoghq.com/docker-adoption/
https://duo.com/blog/state-of-the-auth-experiences-and-perceptions-of-multi-factor-authentication
https://venturebeat.com/2018/08/22/global-survey-reveals-low-adoption-of-multi-factor-authentication-for-office-365/
https://fidoalliance.org/wp-content/uploads/The-State-of-Authentication-Report.pdf

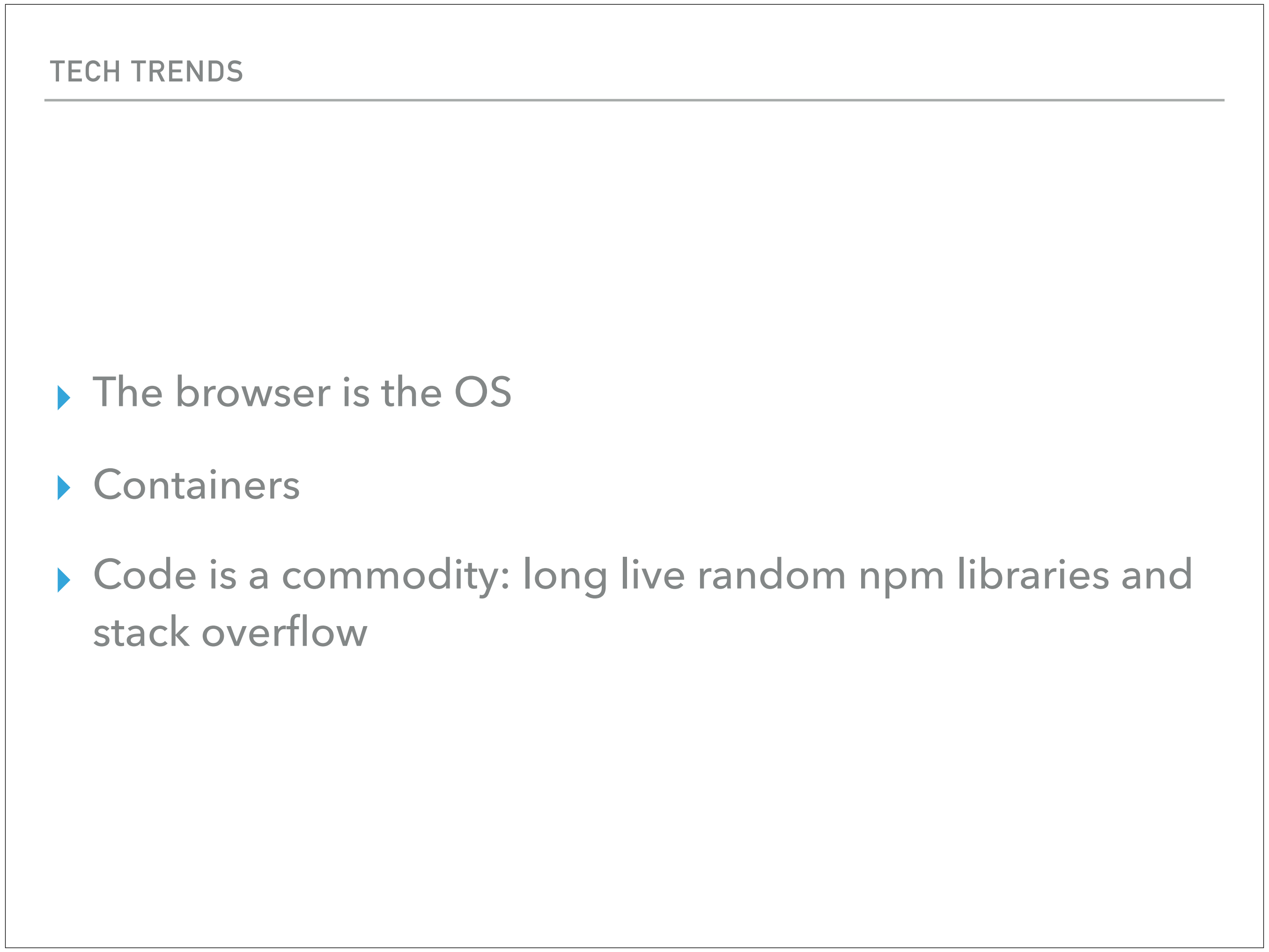


SO WHERE IS THE INDUSTRY HEADED?

Offense is the most explanatory variable of the whole industry and offense will have to change

A sometimes forgotten fact is that infosec is inherently reactive, wherever offense scales defense has to perform (new) work and hence shape the type of people we hire, the focus we have etc etc.

Also in general, robust offense is borne out of architectural mistakes creeping in ubiquitous technology



TECH TRENDS

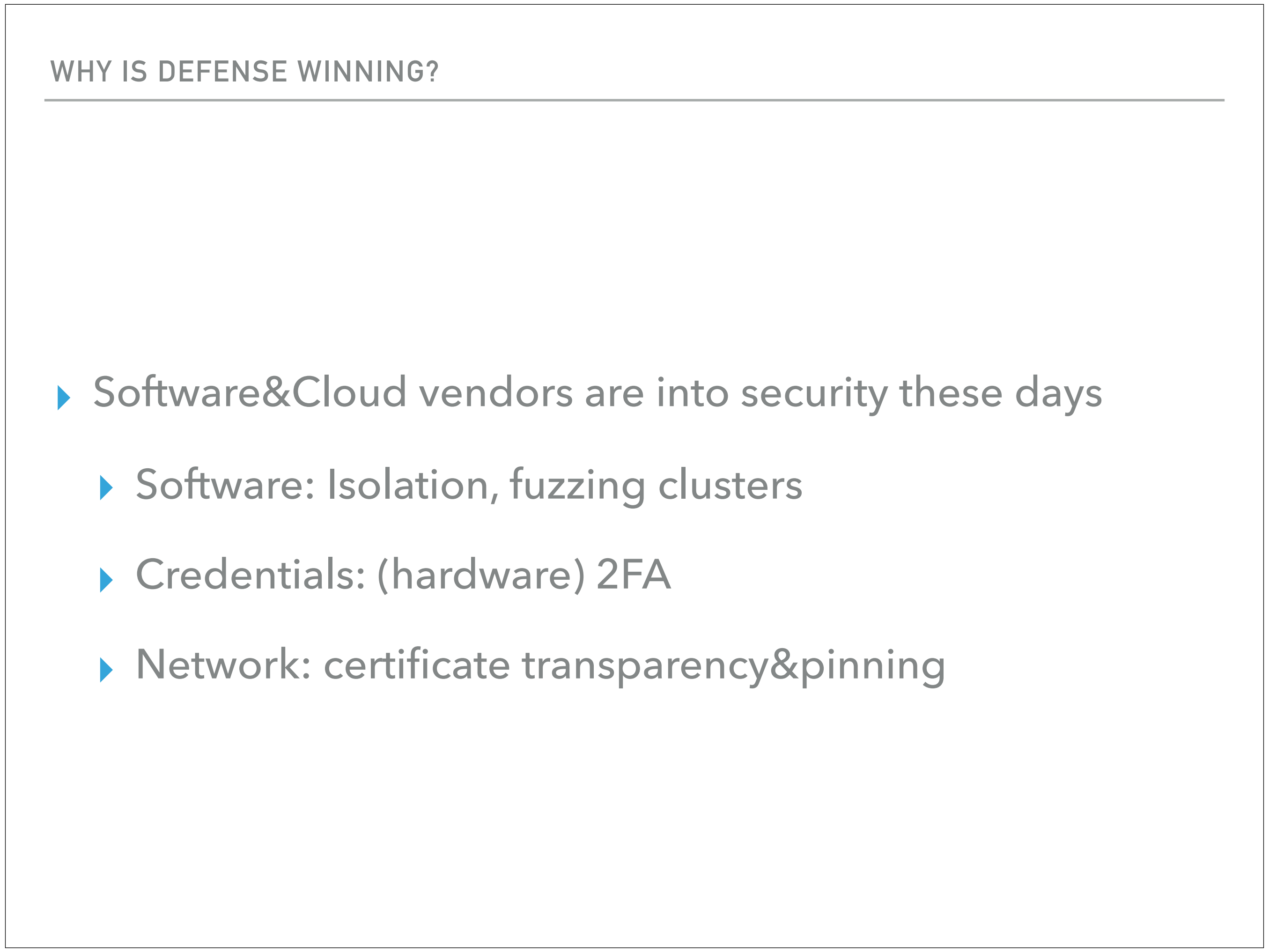
- The browser is the OS
- Containers
- Code is a commodity: long live random npm libraries and stack overflow

It’s not just innovation on the defensive side, the broader tech trends helped a lot in securing things..

A new OS (browsers and phones) means the opportunity to restructure security posture. As an example, browsers are forcefully deprecating bad behavior (flash, java, non-TLS).

Containers give more control to cloud providers and big tech vendors who now care about security.

Containers also help massively in reducing persistence capabilities



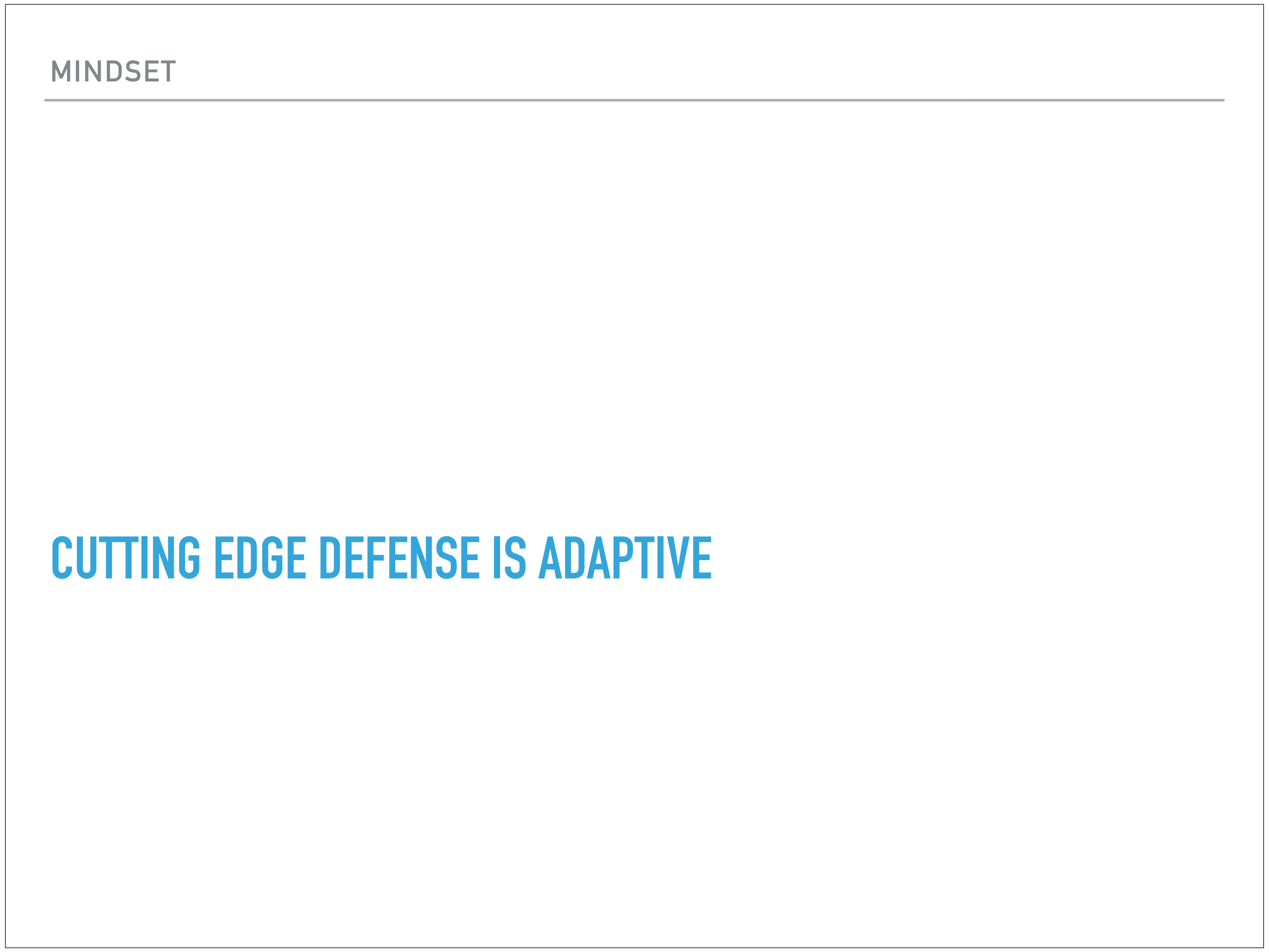
WHY IS DEFENSE WINNING?

- Software&Cloud vendors are into security these days
  - Software: Isolation, fuzzing clusters
  - Credentials: (hardware) 2FA
  - Network: certificate transparency&pinning

We have developed the technology to potentially mitigate/reduce the damage of the vast majority of attacks we know of today. On top of that, there seems to be enough momentum for adoption of most of this tech (see earlier slide).

I believe the single most important change in the industry is that software&cloud vendors (mostly FAANG (+MSFT) and Chinese equivalent) have prioritized security by aggressively hiring offensive people and “over” hiring in security in general. The end result is that we have now architected systems that can cope well with the most well known attack patterns of the past decade.

Hardware-based 2FA makes phishing harder, certificate pinning&transparency make MITM and similar attacks much harder



MINDSET

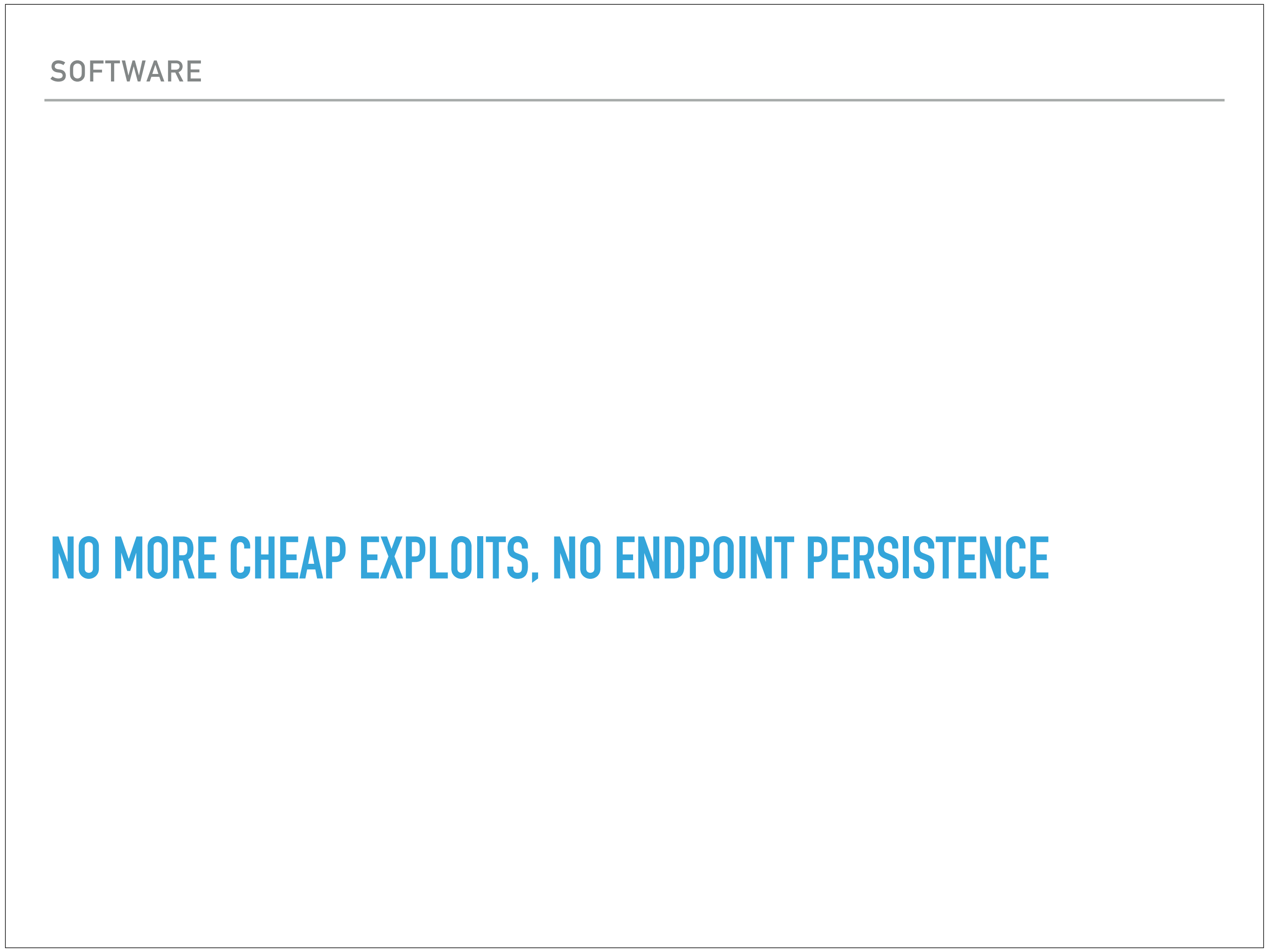
CUTTING EDGE DEFENSE IS ADAPTIVE

Whether it’s your next gen endpoint company/MSSP or your best in class tech company, defense is less monolithic and reactive than it used to be. We observe this both at the “software level” (aka you can’t easily find mutation of old bugs or techniques anymore) but more in general as a mindset shift.

The new focus tends to be on the adversary more than on the tools used by the adversary, this makes detection time and efficacy much higher.

Arguably Snowden was one of the driving forces behind this, together with the inability of security vendors to detect most of the APTs we saw: https://www.wired.com/2012/06/internet-security-fail/

Snowden was a wake up call in terms of realizing that (1) there's more offensive stuff going on than previously thought (2) it's not commoditized off-the-shelf malware (3) showing how it was done helped focusing on the right area. (4) Snowden partially caused
intel agencies to go "defensive" and so you have more work like this: https://www.ncsc.gov.uk/information/active-cyber-defence-one-year



SOFTWARE

NO MORE CHEAP EXPLOITS, NO ENDPOINT PERSISTENCE

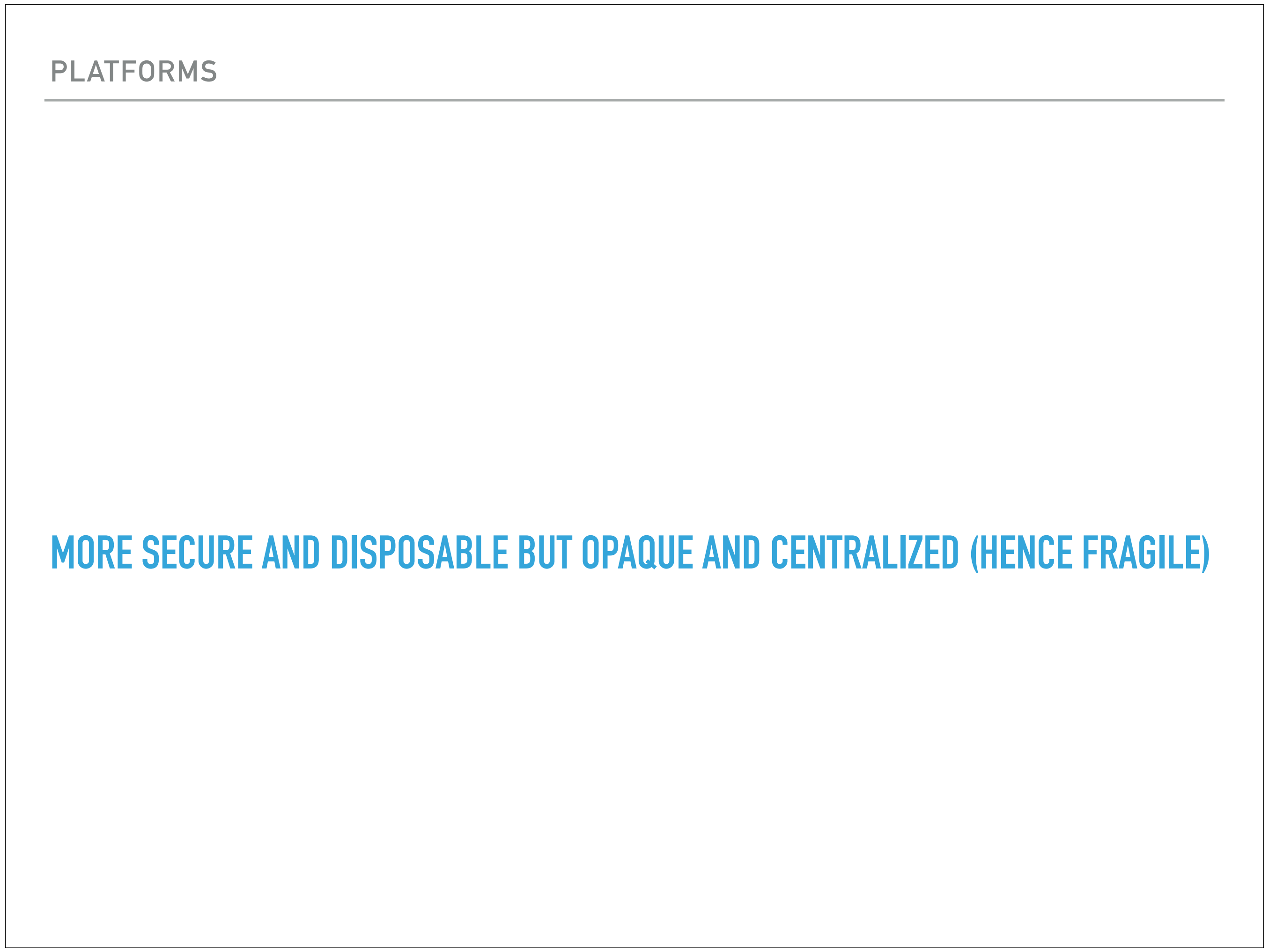
Ever stricter sandboxes + massive fuzzing clusters

Hardware-based mitigations on the horizon

Containers = flip back to known-good states

Code attestation (code-signing et al)

IoT/dumber devices still highly vulnerable but different type of access and capabilities



PLATFORMS

MORE SECURE AND DISPOSABLE BUT OPAQUE AND CENTRALIZED (HENCE FRAGILE)

Harder to persist, perform lateral movement and in general perform offensive research.

But it’s not all good, yes we are more secure on the other hand it is more centralized and hence more fragile:
1) Repositories of “clean-state” images and code is single point of failure
2) Software vendors doing security means less incentive for accessible platforms
3) Code-signing and so forth relies on PKI infrastructure
4) We really have no visibility over the cloud architecture and how secure the architecture really is

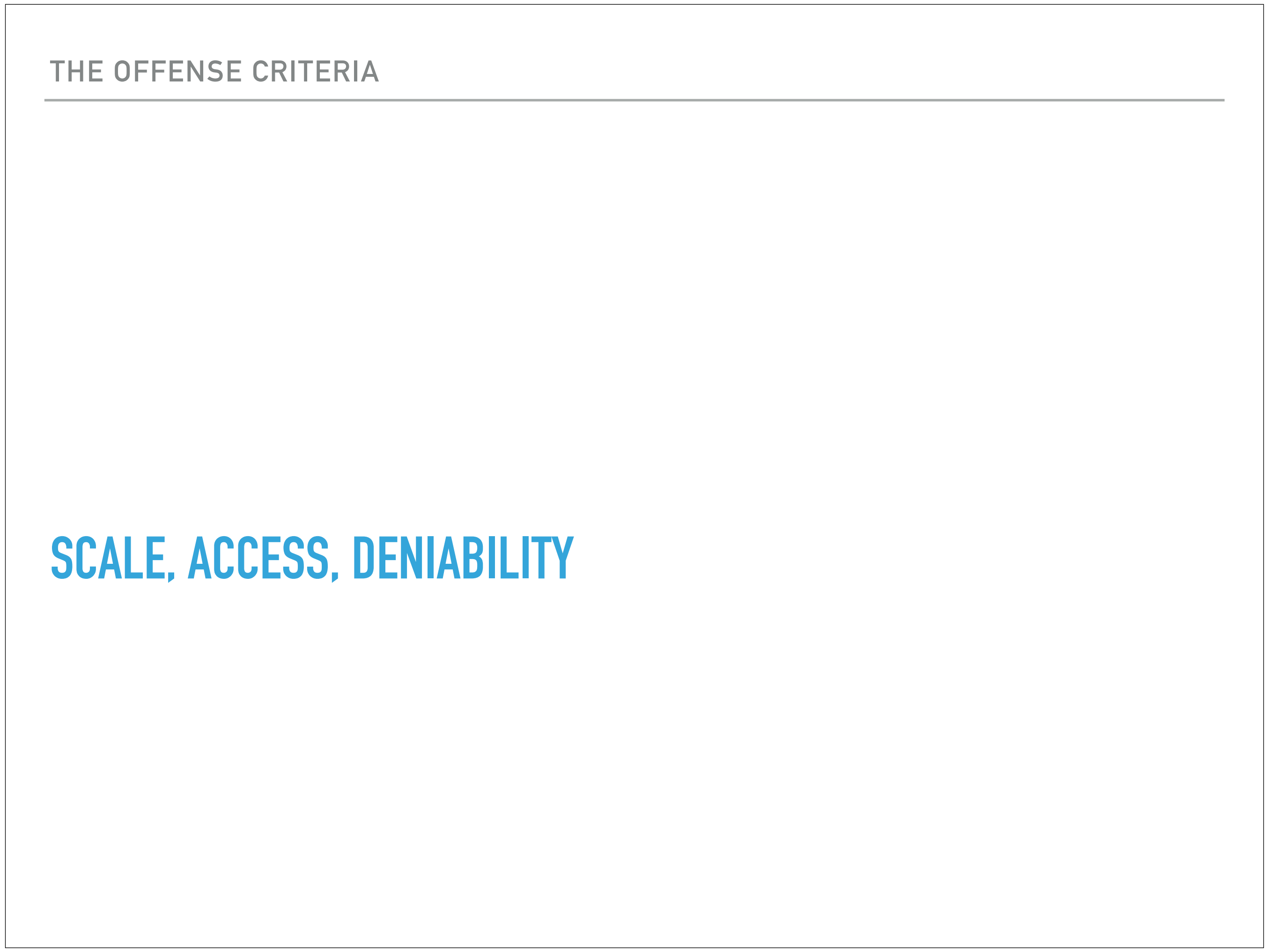
TIME TO GO HOME?

No, offense in current form (think stuxnet-like campaigns) will always exist - it will just not be as scalable(no more “point and click” solutions). Are there other areas where to scale instead?

WHERE IS OFFENSE GOING?

CREDS, DIGITAL CRITICAL INFRASTRUCTURE AND SOCIAL ENGINEERING

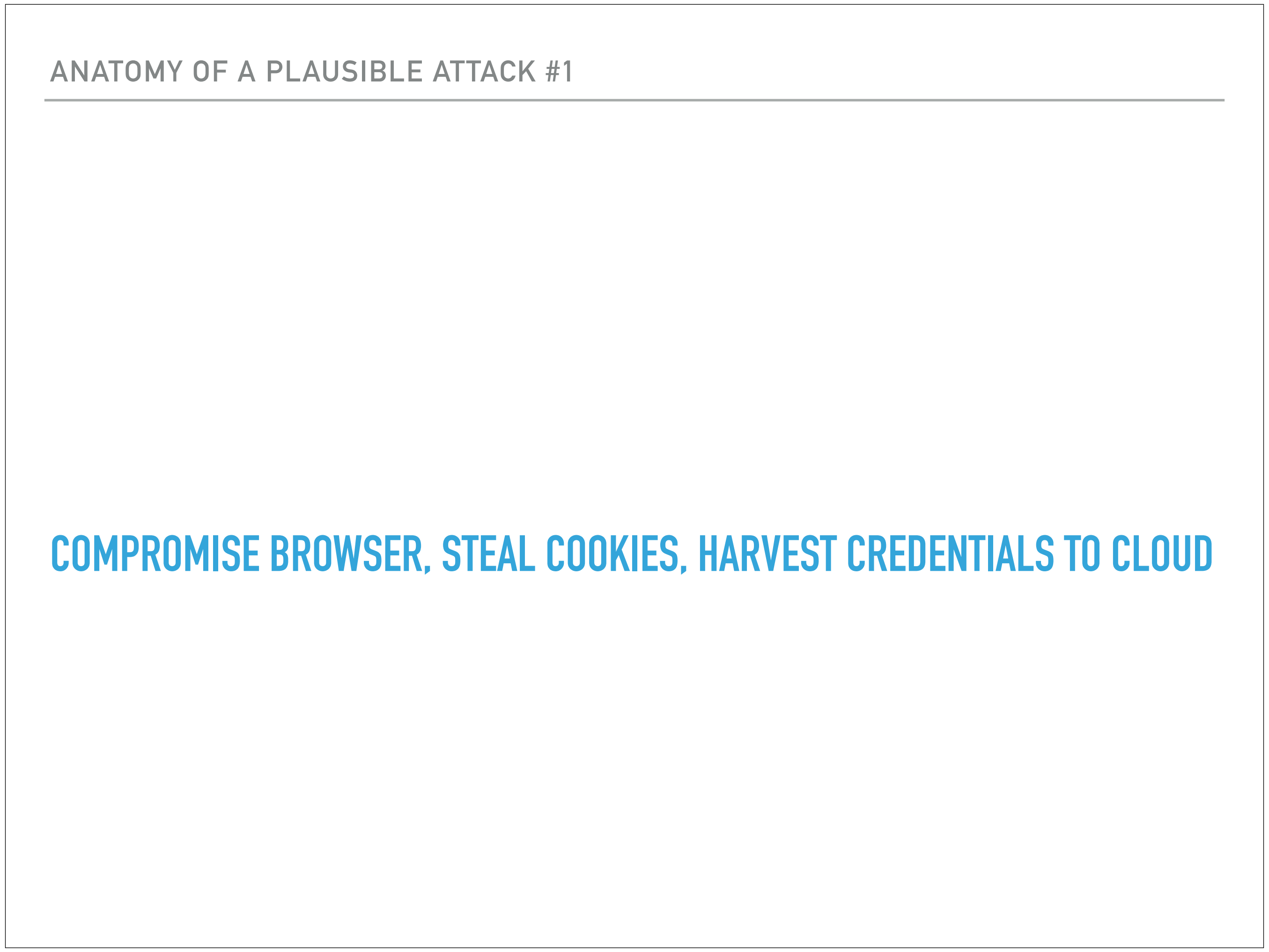
Let’s keep in mind that today you can phish your way into anything…



THE OFFENSE CRITERIA

SCALE, ACCESS, DENIABILITY

You want easy to perform attacks, that are as generic as possible and easiest to deny, and that give you the most access



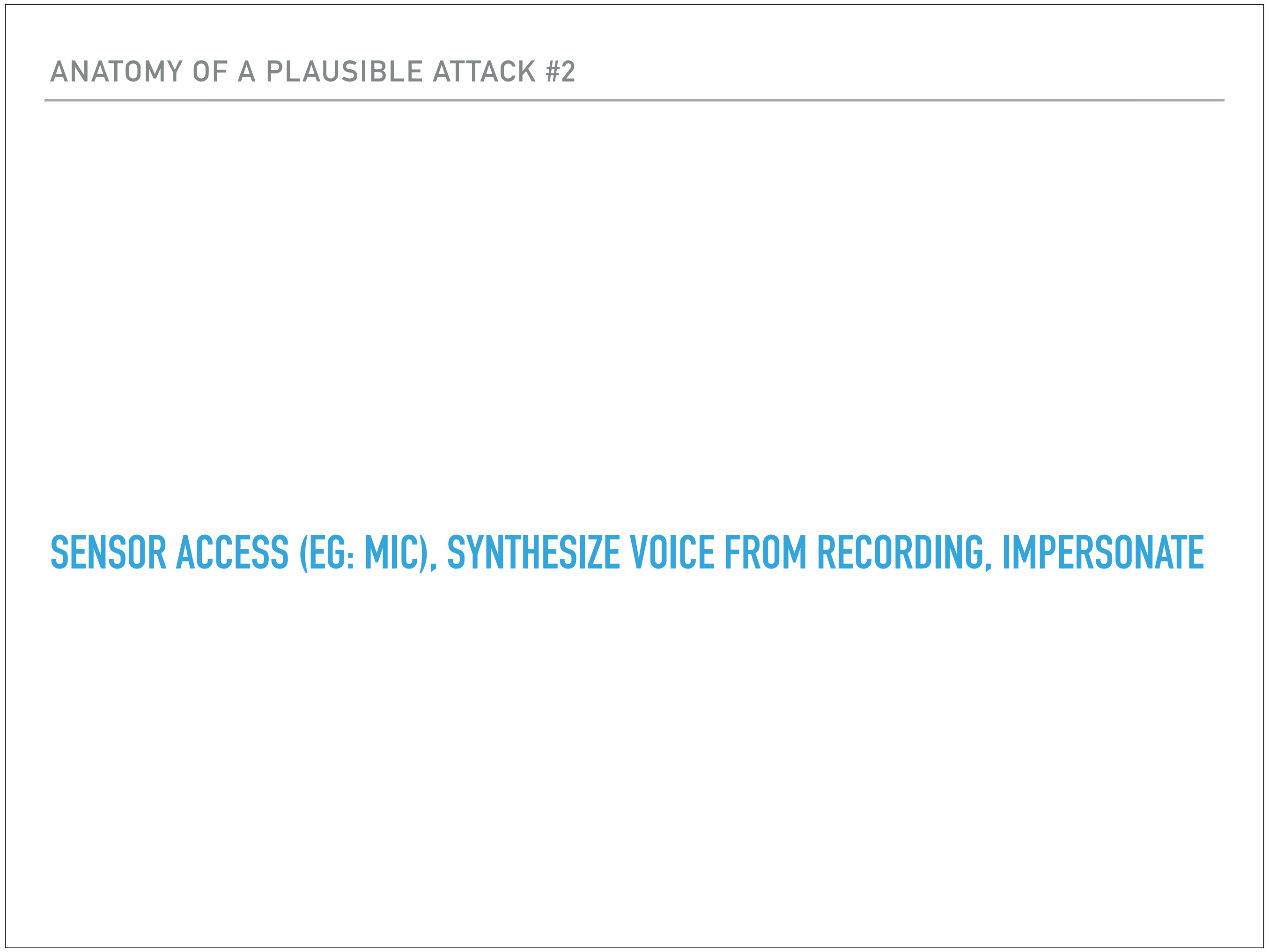
ANATOMY OF A PLAUSIBLE ATTACK #1

COMPROMISE BROWSER, STEAL COOKIES, HARVEST CREDENTIALS TO CLOUD

Compromise the renderer, obtain persistence in the renderer process

“Lateral movement” with cookies/credentials.

Criteria: Generic&deniable



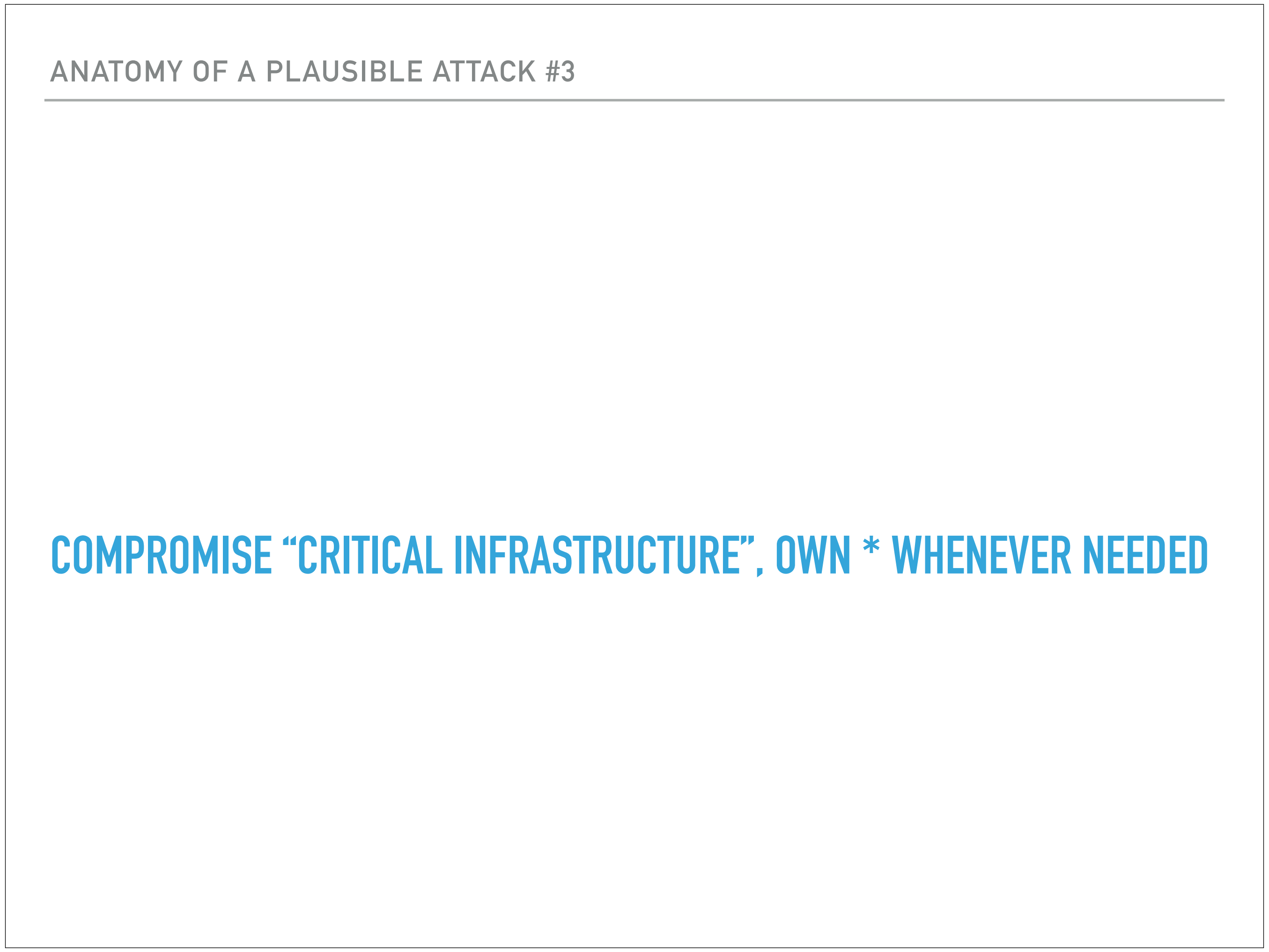
ANATOMY OF A PLAUSIBLE ATTACK #2

SENSOR ACCESS (EG: MIC), SYNTHESIZE VOICE FROM RECORDING, IMPERSONATE

This is the “social engineering” part, we have the technology to create fake voices and videos. Even in the absence of technology, much easier to social engineer your way through something if you have eyes and ears on a person.

Attackers will soon use this for fraud and similar attacks

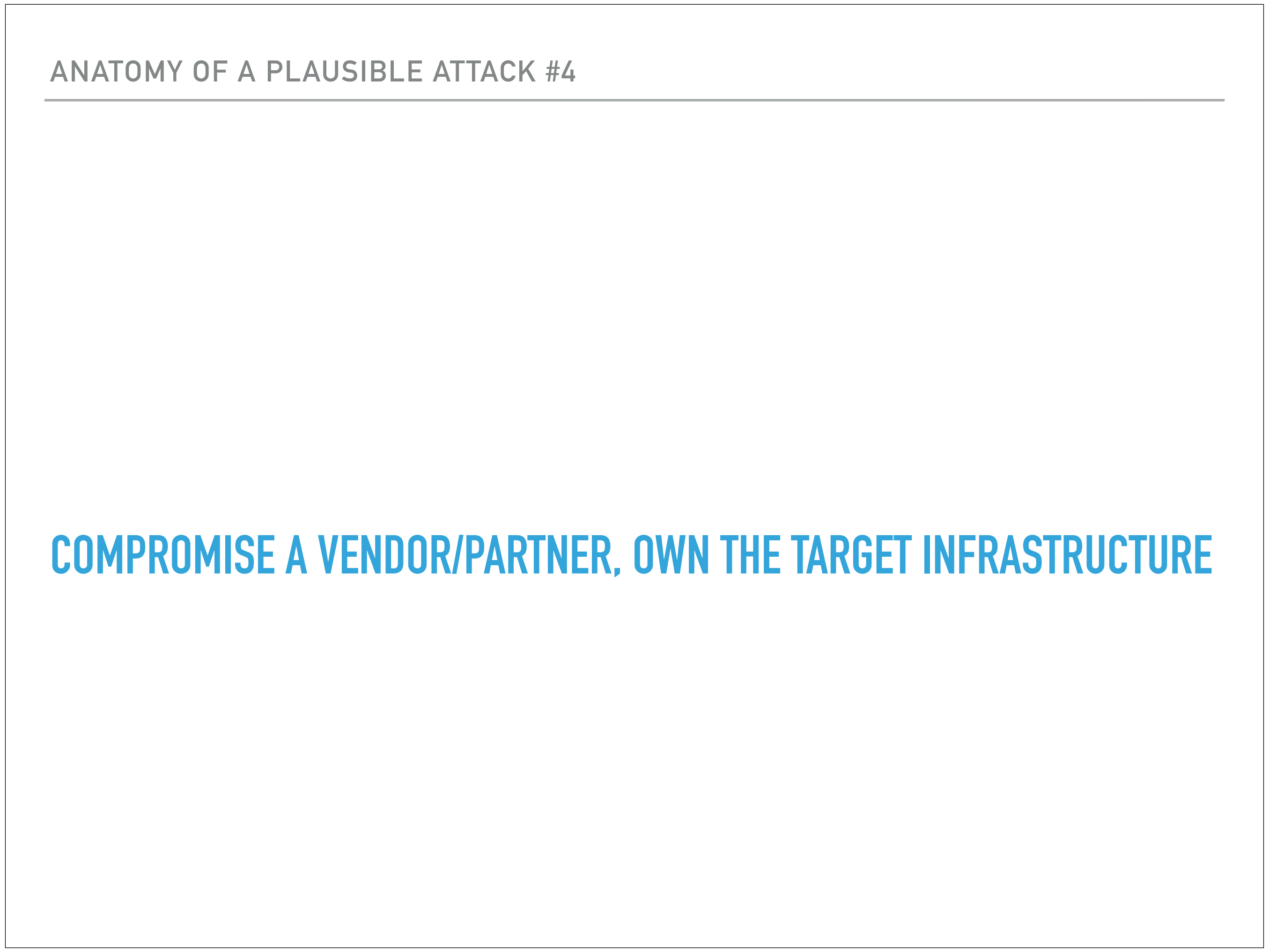
Criteria: Scale&deniability



ANATOMY OF A PLAUSIBLE ATTACK #3

COMPROMISE “CRITICAL INFRASTRUCTURE”, OWN * WHENEVER NEEDED

Criteria: scale&access

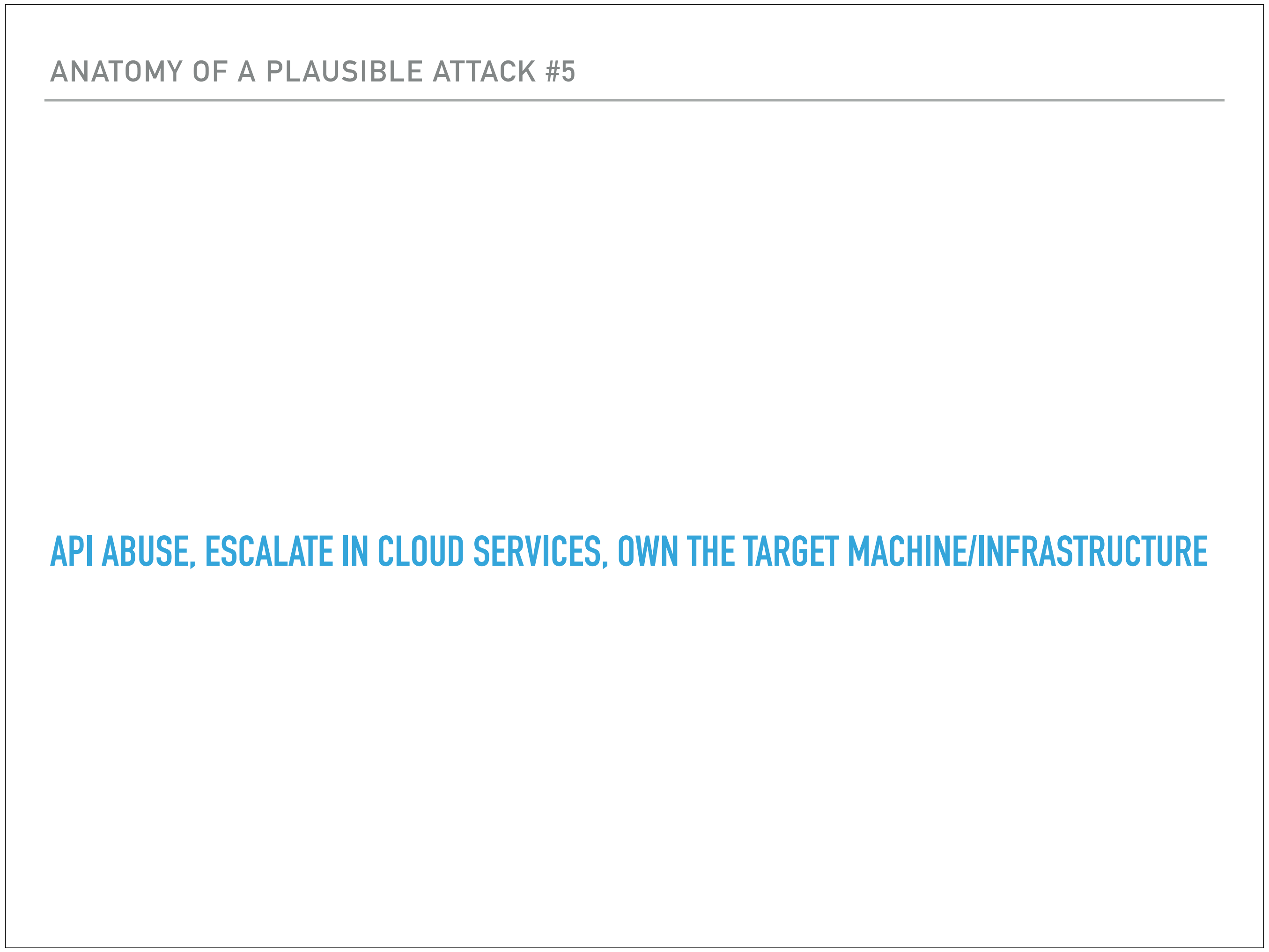


ANATOMY OF A PLAUSIBLE ATTACK #4

COMPROMISE A VENDOR/PARTNER, OWN THE TARGET INFRASTRUCTURE

So many examples of this already today.. Pretty much every attention-grabbing data breach of the past few years was a variation of this

Criteria: access&scale&deniability



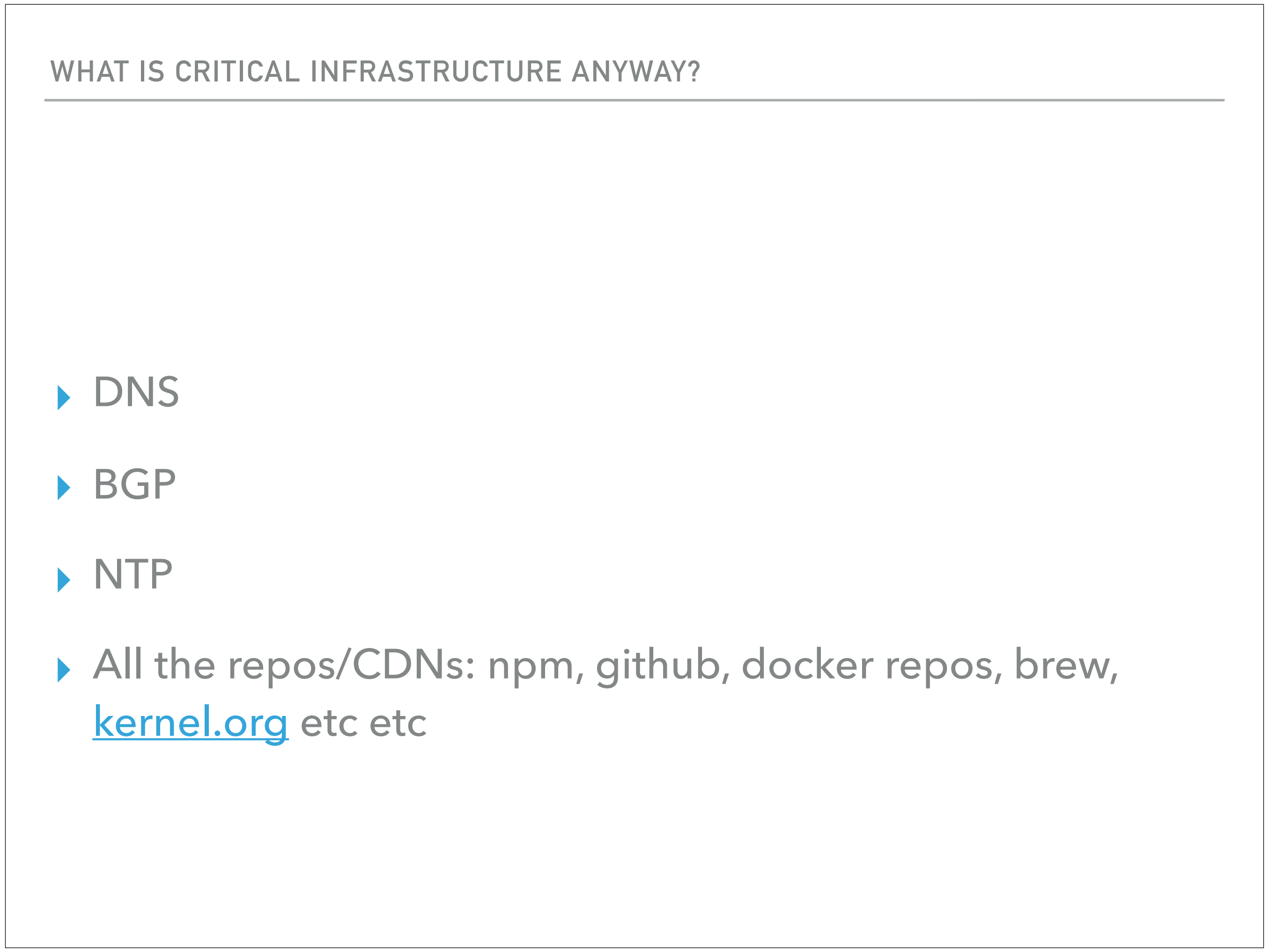
ANATOMY OF A PLAUSIBLE ATTACK #5

API ABUSE, ESCALATE IN CLOUD SERVICES, OWN THE TARGET MACHINE/INFRASTRUCTURE

This is probably one of the best patterns for an attacker given the simplicity. We are starting to see some of this today already.

Again, in general the cloud is a complete blackbox from a security standpoint and we are getting closer and closer to “programming” your networking environment. At the same time we don’t have the tools or knowledge to debug/audit and test these new programming paradigms.

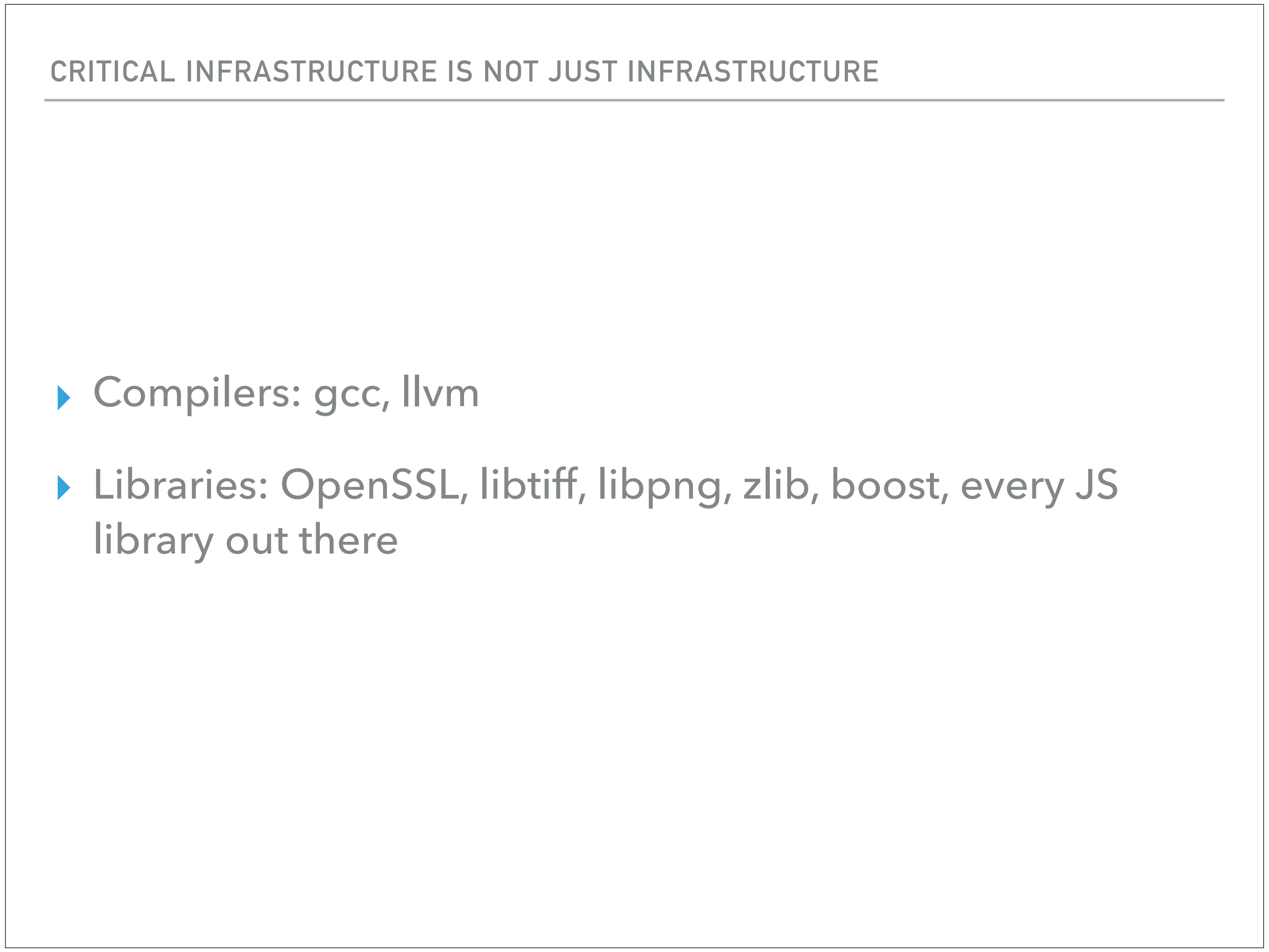
Criteria: access&deniability



WHAT IS CRITICAL INFRASTRUCTURE ANYWAY?

- DNS
- BGP
- NTP
- All the repos/CDNs: npm, github, docker repos, brew, kernel.org etc etc

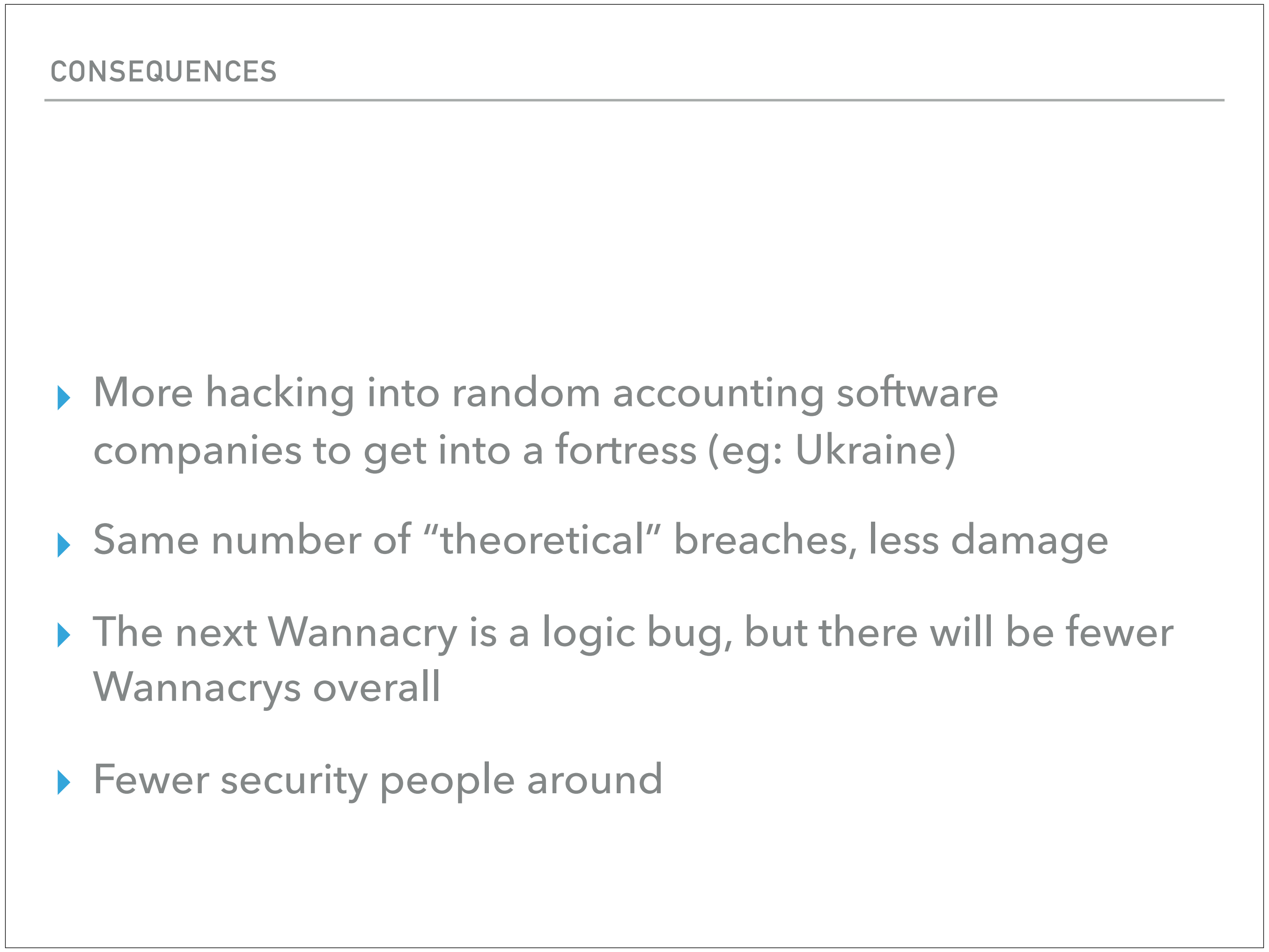
Most of this infrastructure is either open source or maintained by orgs with very limited funding.



CRITICAL INFRASTRUCTURE IS NOT JUST INFRASTRUCTURE

- Compilers: gcc, llvm
- Libraries: OpenSSL, libtiff, libpng, zlib, boost, every JS library out there

Let’s keep in mind that we still have no idea how to properly analyze code. Most of these libraries are community-maintained and open source. OSS fuzzing and similar initiatives are trying to help with securing these but obviously it’s not enough and it’s not architectural.



CONSEQUENCES

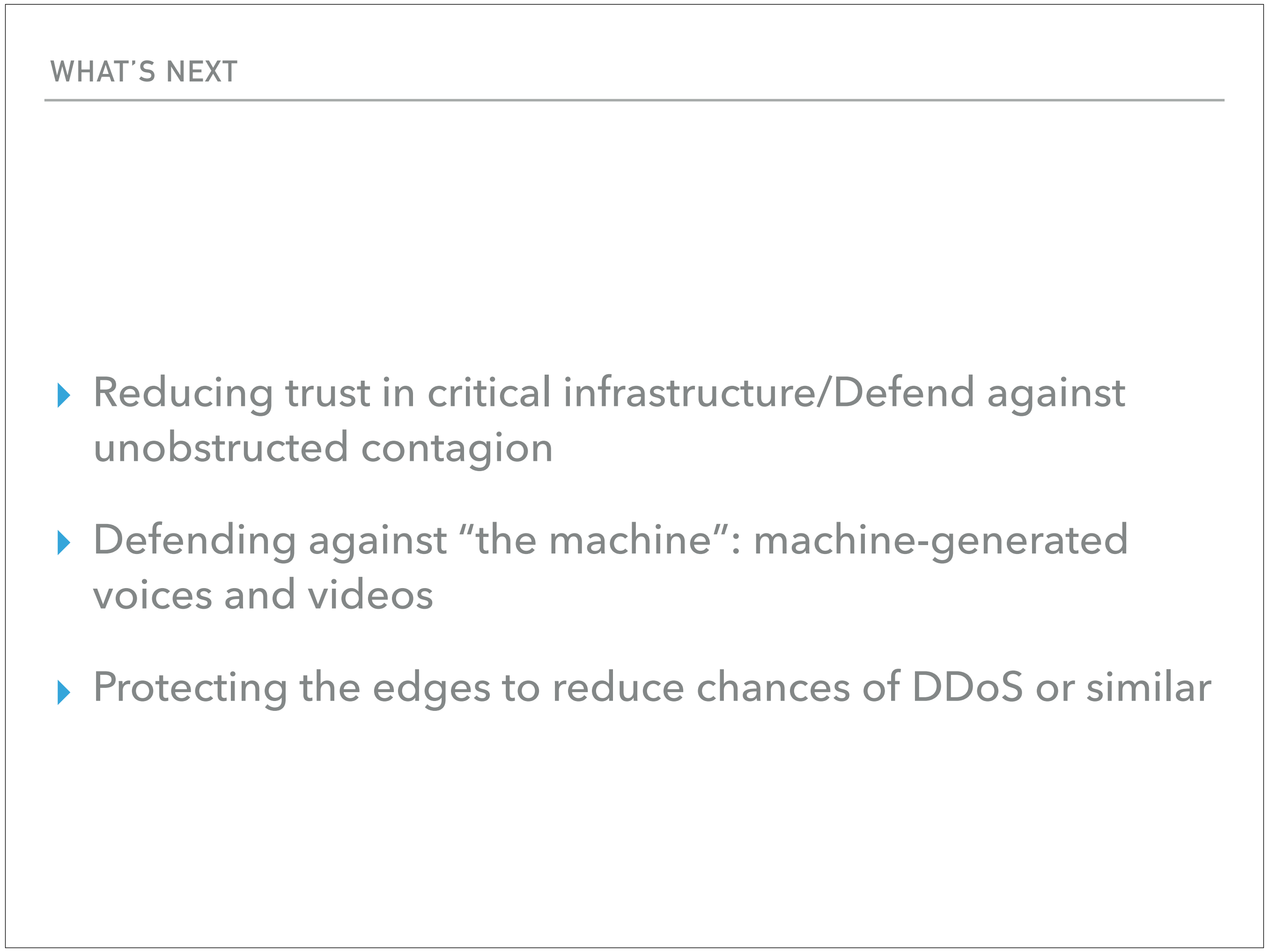
- More hacking into random accounting software companies to get into a fortress (eg: Ukraine)
- Same number of “theoretical” breaches, less damage
- The next Wannacry is a logic bug, but there will be fewer Wannacrys overall
- Fewer security people around

This is not news: hacking into less-protected stuff to get into more protected orgs has been happening for years

Maybe the average rate of compromised machines will stay the same but the damage caused will be much lower due to isolation, inability to persist etc etc.

Wormable attacks against non-IoT devices are going to become rarer and rarer

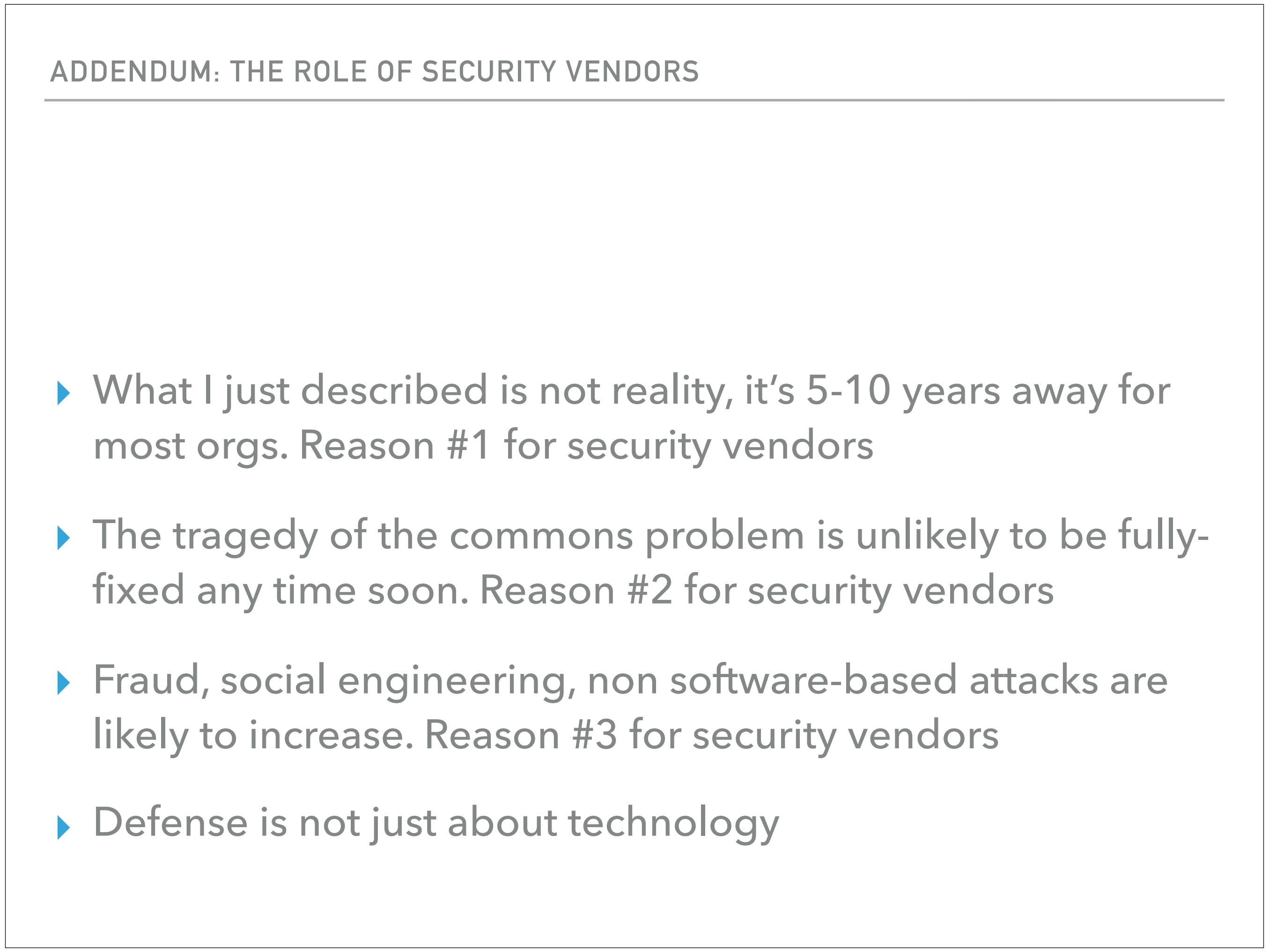
Hacking critical infrastructure means everyone is within reach yet nobody wants to lose access -> less visible attacks and damage



WHAT’S NEXT

- Reducing trust in critical infrastructure/Defend against unobstructed contagion
- Defending against “the machine”: machine-generated voices and videos
- Protecting the edges to reduce chances of DDoS or similar

Open problems

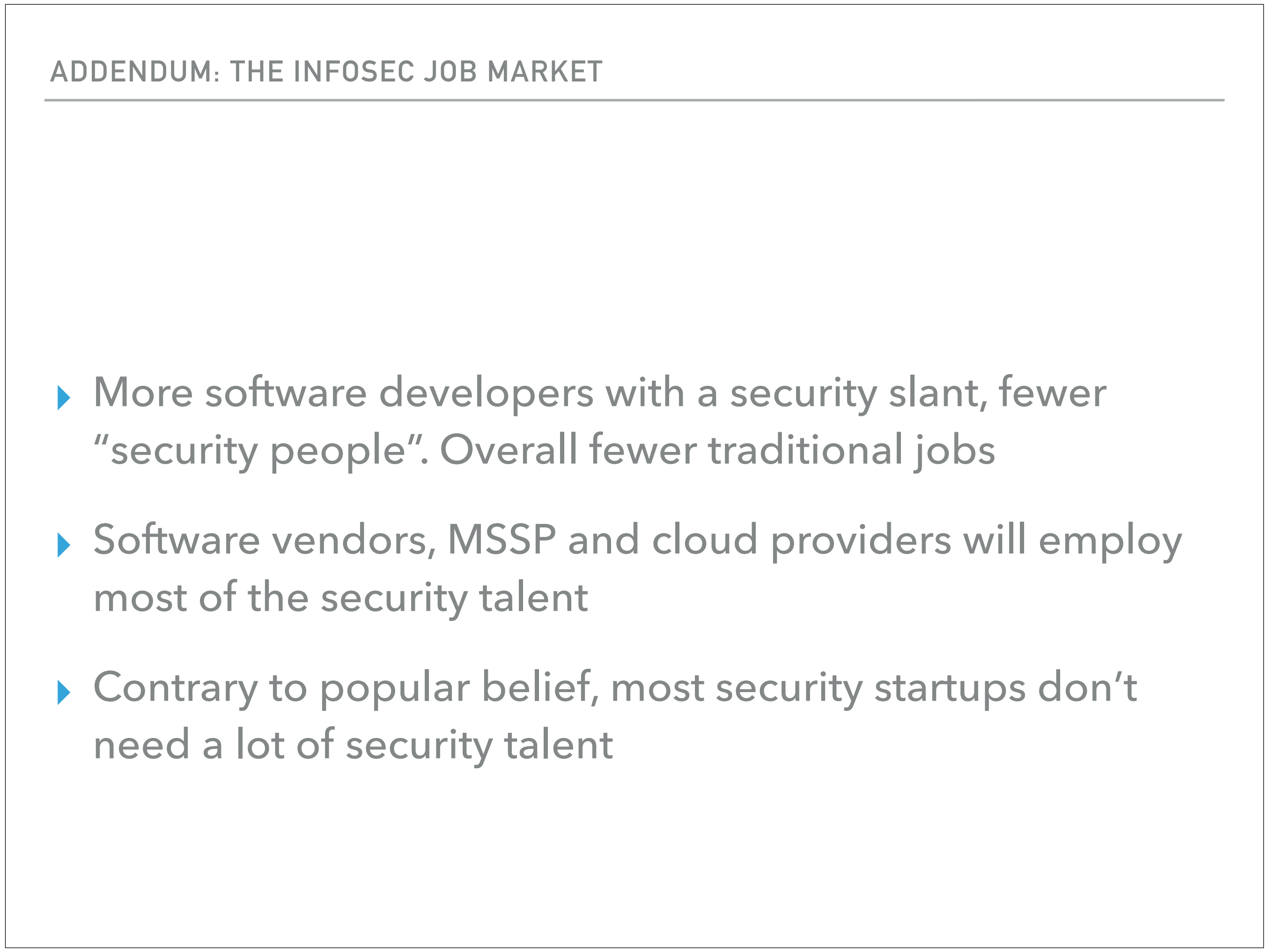


ADDENDUM: THE ROLE OF SECURITY VENDORS

- What I just described is not reality, it’s 5-10 years away for most orgs. Reason #1 for security vendors
- The tragedy of the commons problem is unlikely to be fully-fixed any time soon. Reason #2 for security vendors
- Fraud, social engineering, non software-based attacks are likely to increase. Reason #3 for security vendors
- Defense is not just about technology

Commons = open source digital critical infrastructure

Defense at scale is not enough and less scale historically is not the business of big tech companies



ADDENDUM: THE INFOSEC JOB MARKET

- More software developers with a security slant, fewer "security people". Overall fewer traditional jobs
- Software vendors, MSSP and cloud providers will employ most of the security talent
- Contrary to popular belief, most security startups don't need a lot of security talent

If you believe that security is becoming more consolidated, then it follows that most firms need to shrink (in relative terms) their security staff.

We are over-hiring security people (pentesters, sysadmin with security expertise etc etc) to fix technical debt, but those levels of employment and wages are not warranted and will be optimized

Security startups need a few "security architects" and a lot of software devs, so that's not the place that absorbs talent

Good security talent will have almost no incentive to start companies because software vendors, MSSP and cloud providers will pay top dollars on a risk adjusted basis

Q&A