Security Through Context and Visibility

Neil Lovering

CCIE #1772

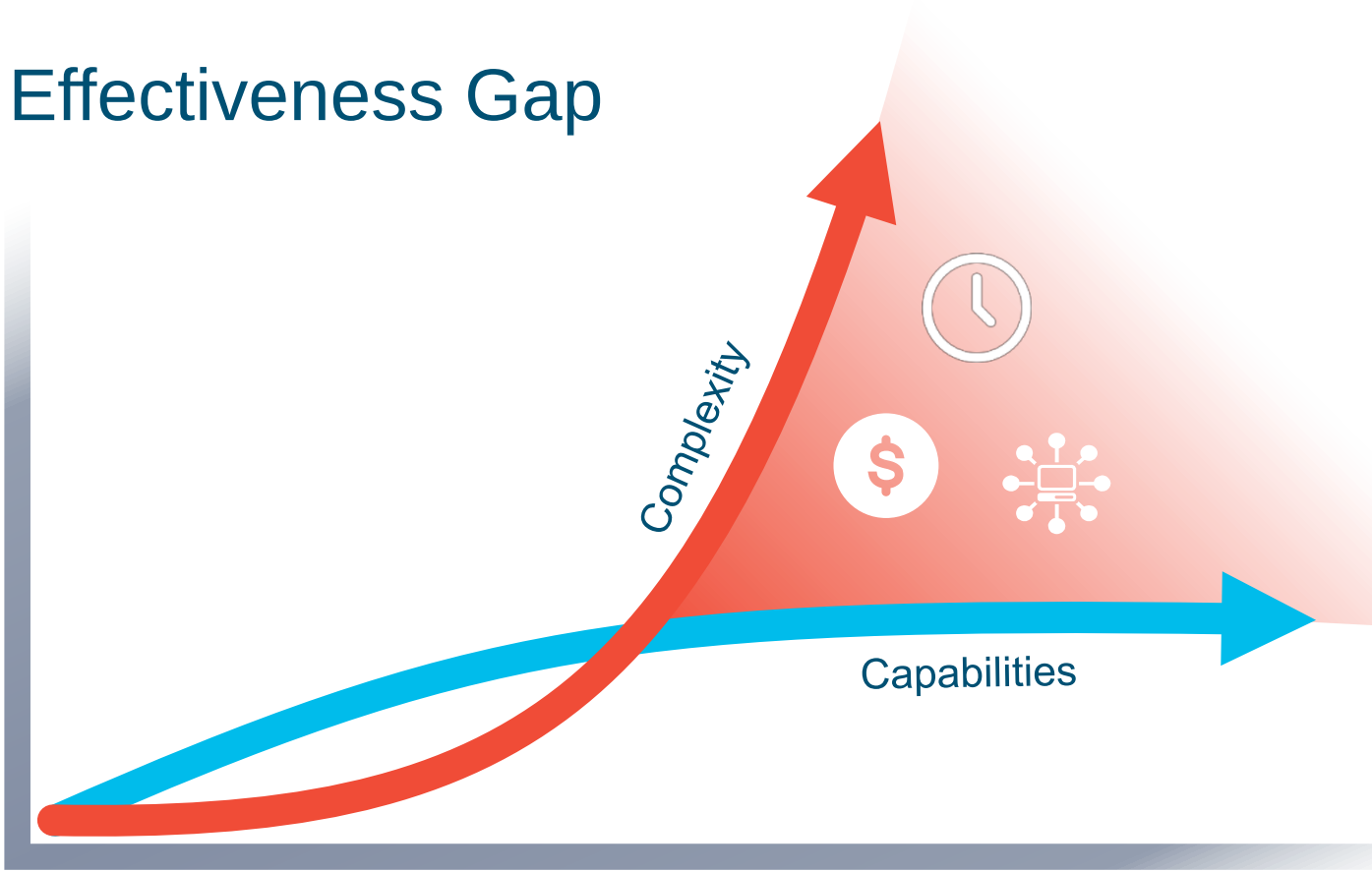
Technical Solutions Architect – Security

How Good is Your Security?

- Not enough?
  - Gaps, holes
  - “Check the box” often does not enhance security
- Too much?
  - No integration or coordination
  - Pet projects
  - User experience
- Proactive or reactive?
  - Prevention and/or Detection alone is not enough
  - You can spend your entire career chasing alerts

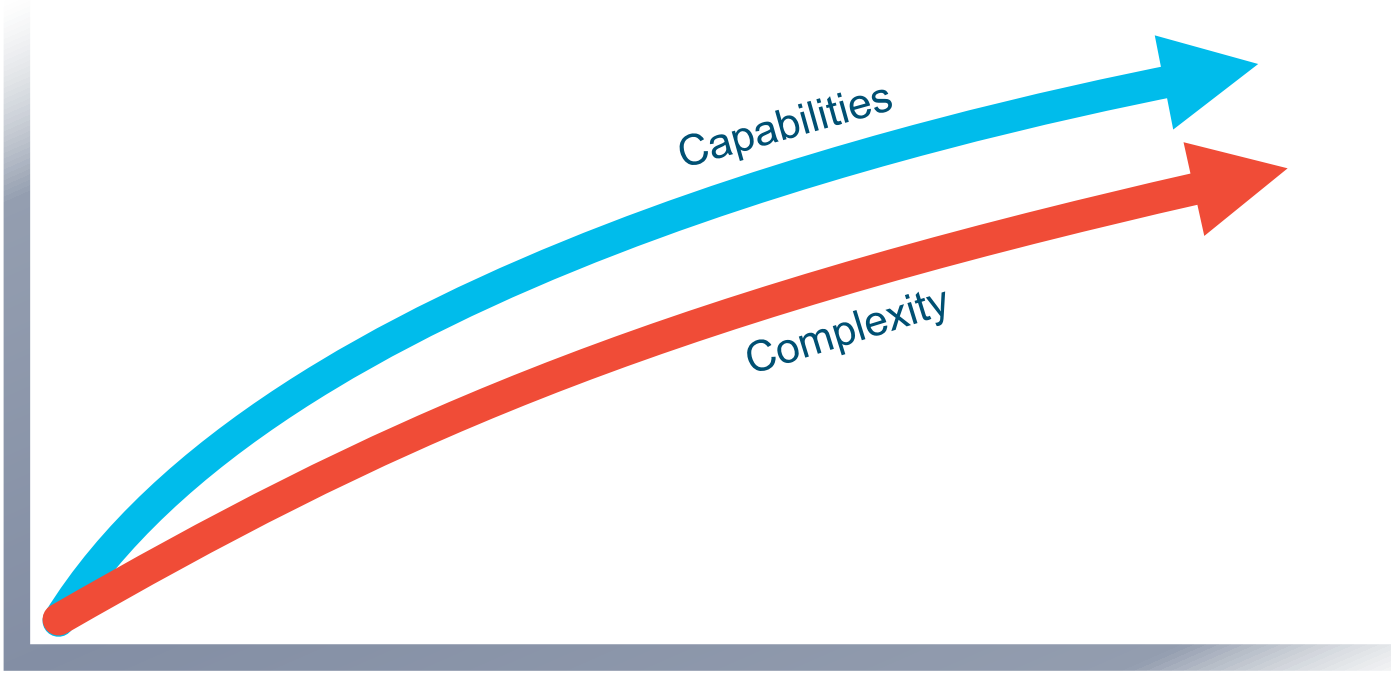
The Security Effectiveness Gap

- Capabilities = What we want
- Complexity = What we do to ourselves
- Time has proven that we have added far too much complexity

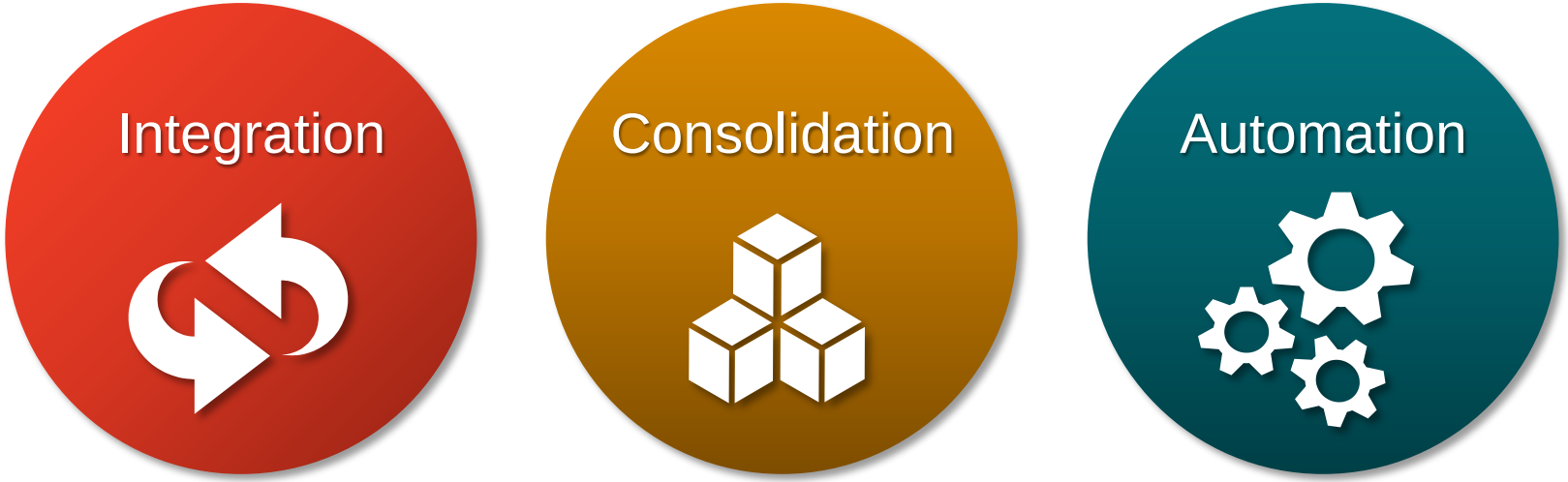


The Goal for Effective Security

- Complexity is expected
  - Multi-vendor / multi-product is typically a challenge
- Complexity must be manageable
- The inability to manage complexity leads to failure



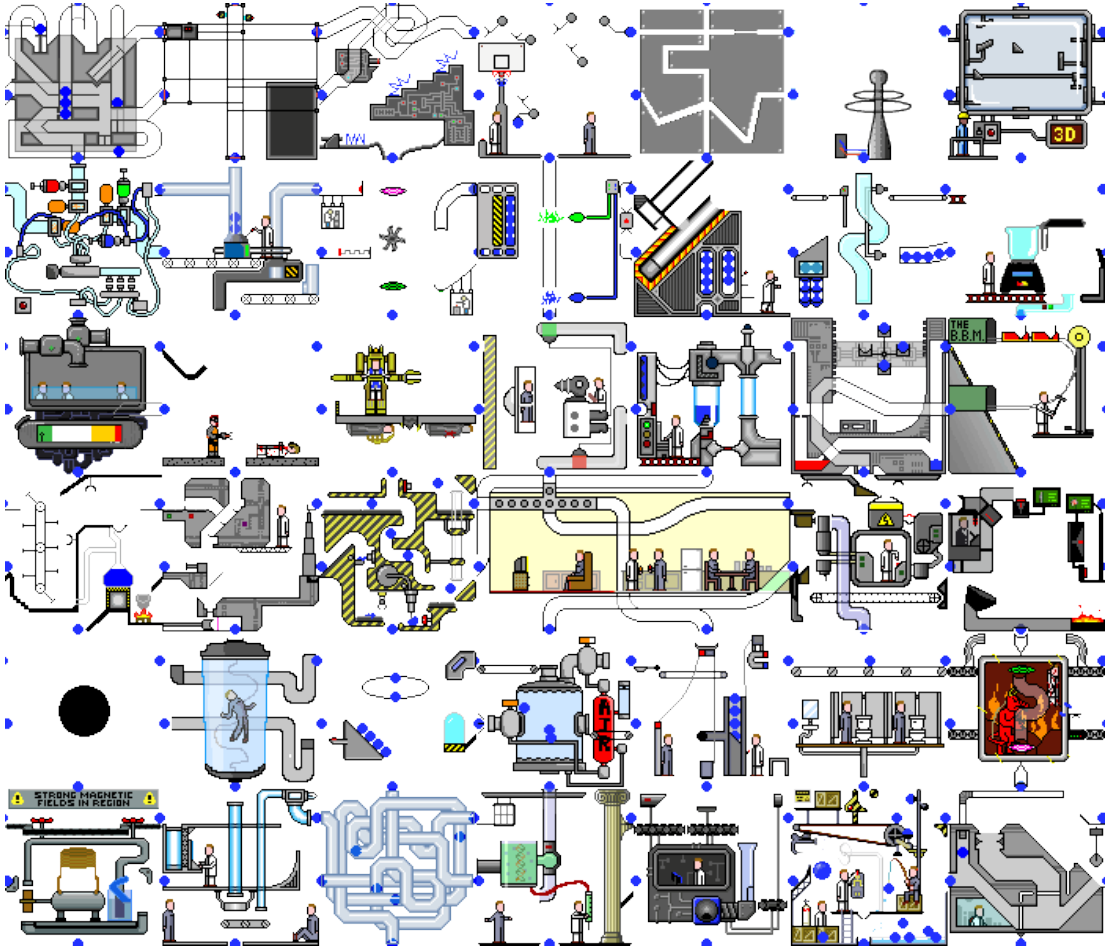
The Path to Effective Security Requires



- Integration, Consolidation and Automation help reduce complexity
- Capabilities do not have to be restricted or limited

Working Together

- Each security product can be complex by itself
- Integration between different security products and vendors is often challenging
- Adding security products to increase capabilities reduces consolidation
- Lack of integration minimizes the effects of automation



Identity Enabled Access – NAC+

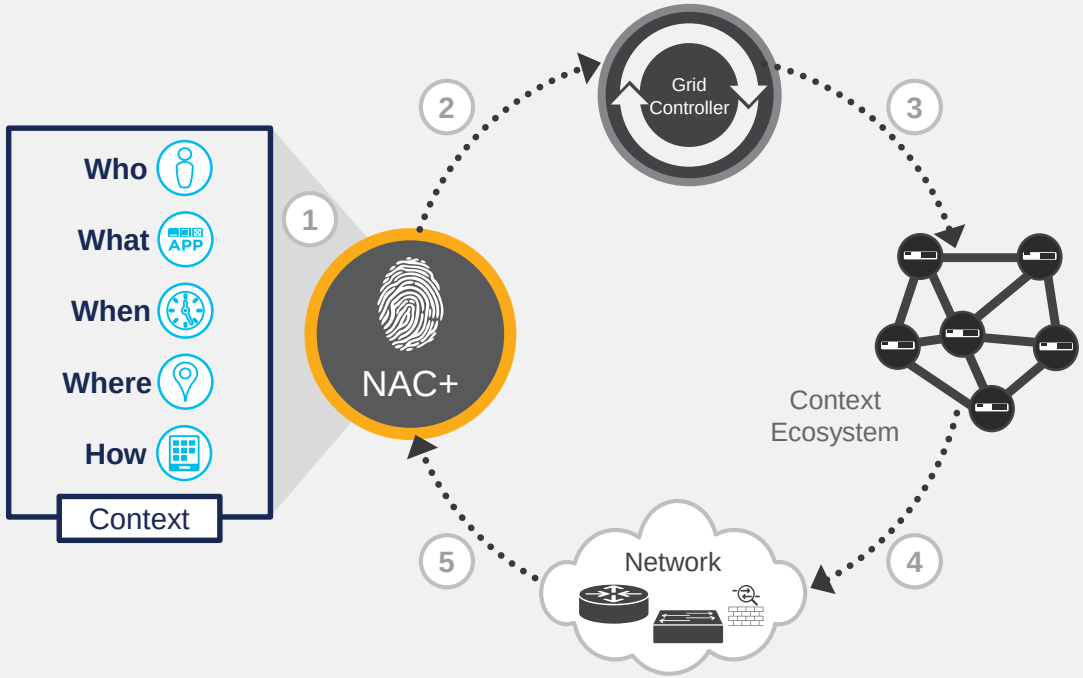
- Keep the good ones in and the bad ones out
- Assess endpoints before network access

WHO	is accessing the network?
WHAT	device is it?
HOW	are they connecting?
WHEN	are they accessing?
WHERE	are they connecting from?
HEALTH	of the endpoint?
THREATS	and vulnerability?

Context aware access control

3 main avenues to access networks:

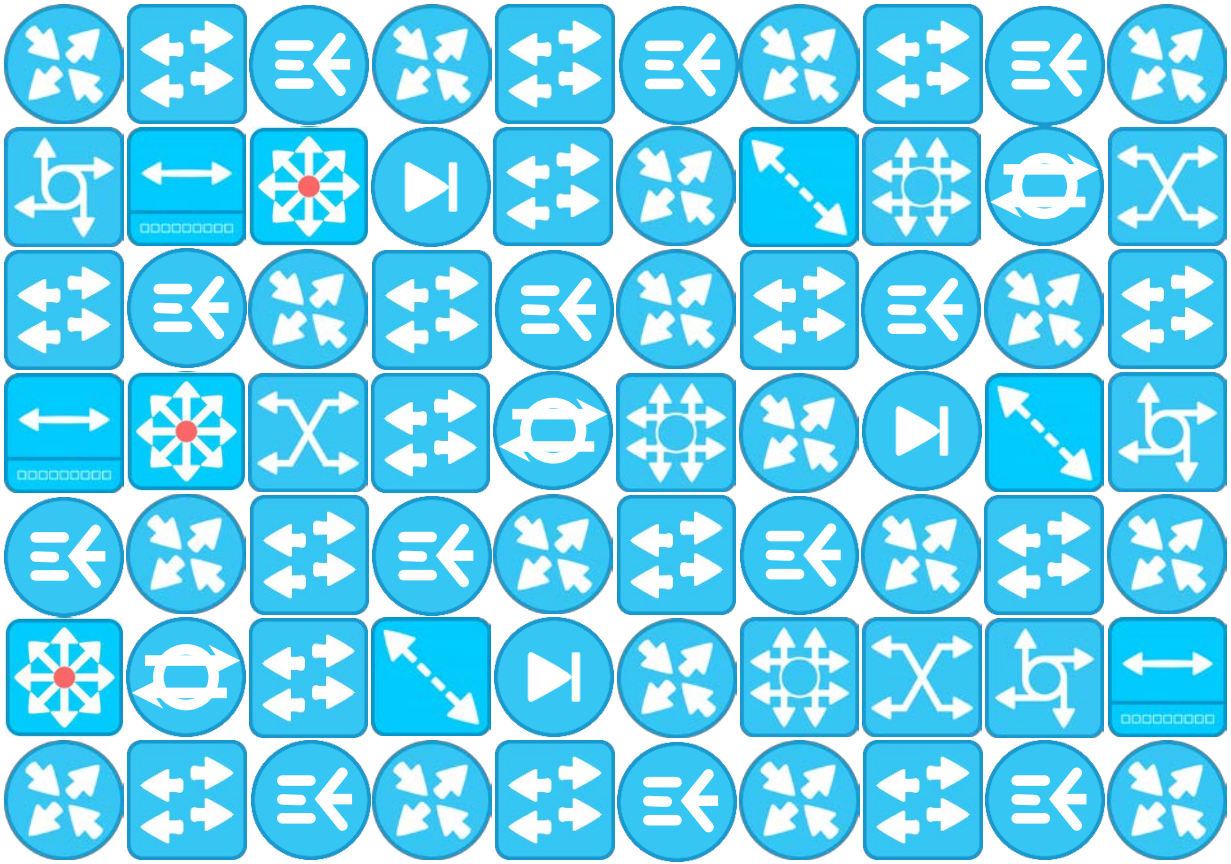
Unified Threat Response by Sharing Contextual Data



1	Collect contextual data from network during NAC
2	Context is shared among security devices
3	Use context to improve visibility to detect threats
4	Direct NAC to rapidly contain threats
5	Use Ecosystem data to update context and refine access policy

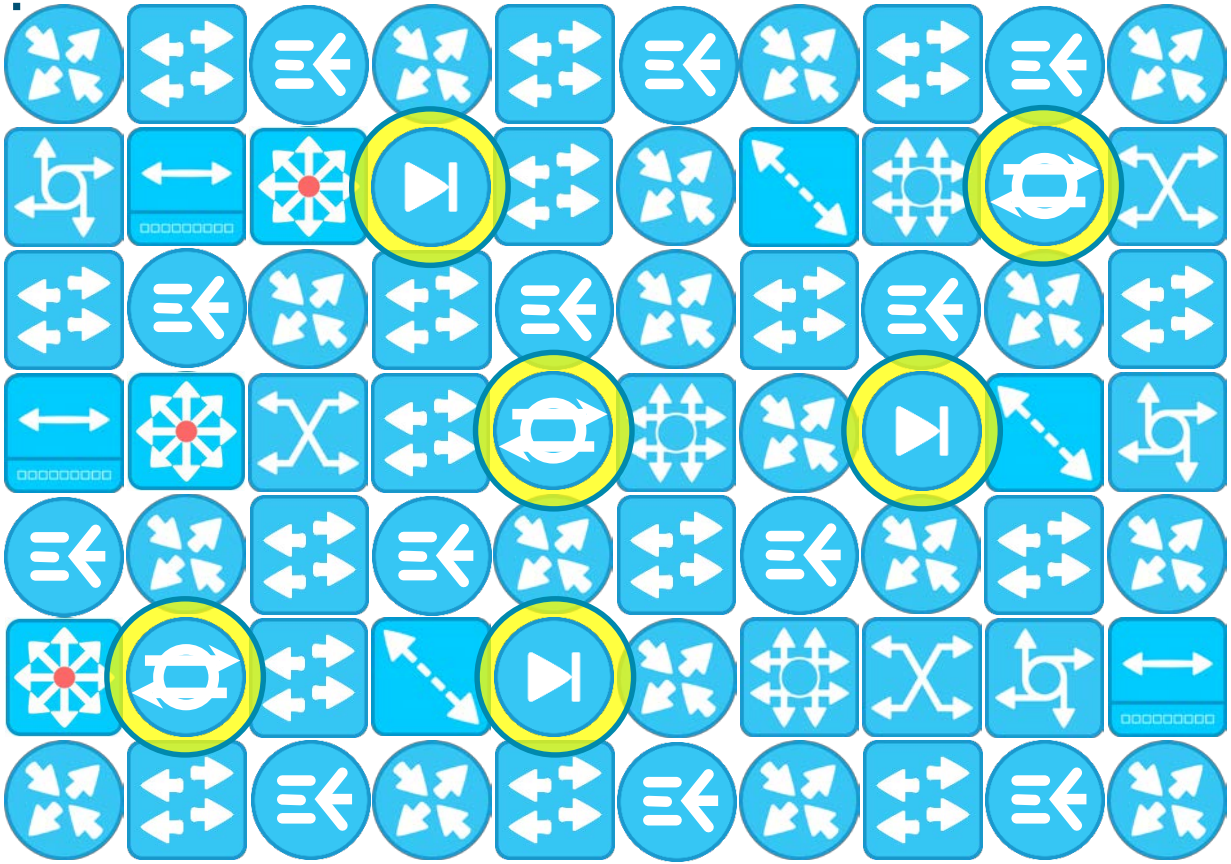
Where’s Waldo?

- Quick – Find the Network Security devices



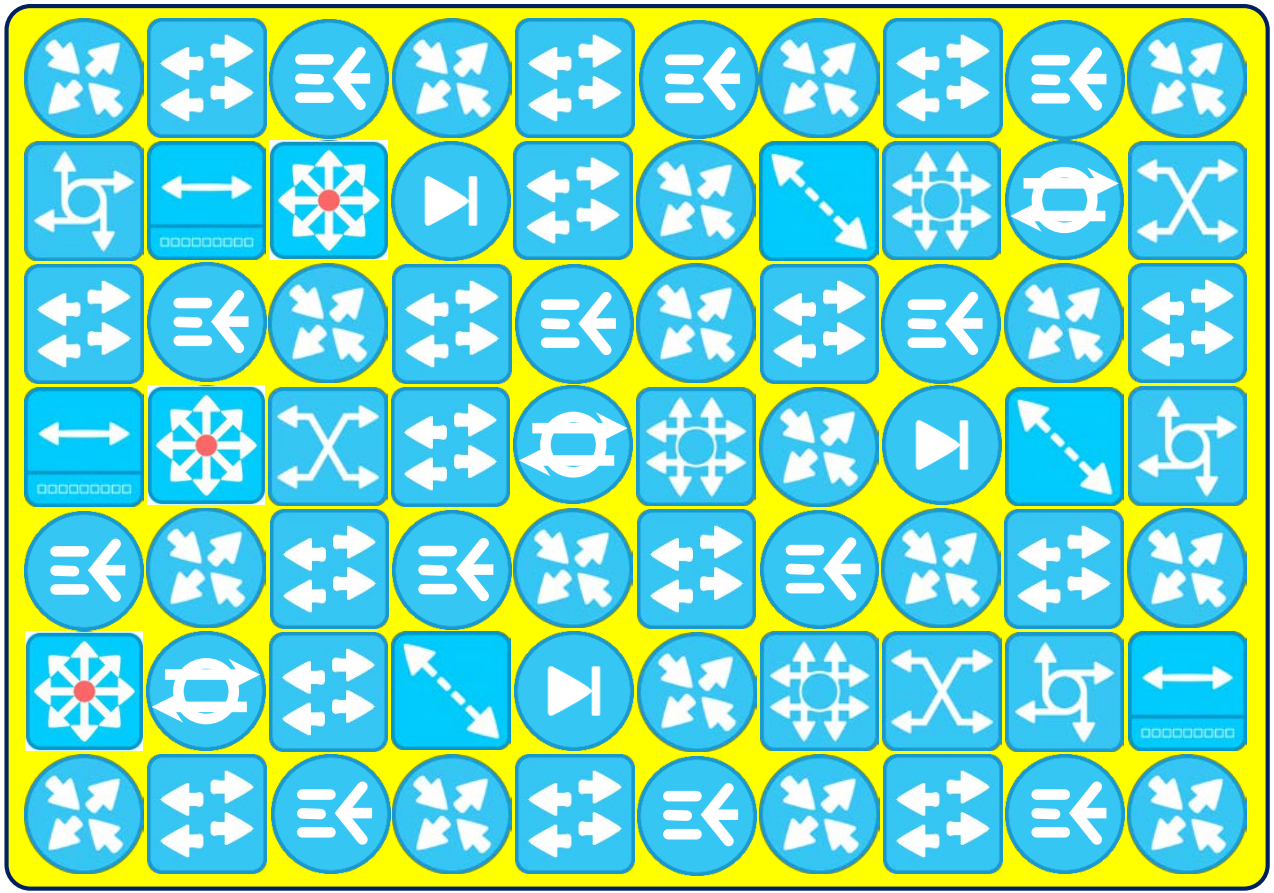
Where's Security?

- Most network devices are *not* security devices
- If you completely depend on security devices for "security", your results may vary



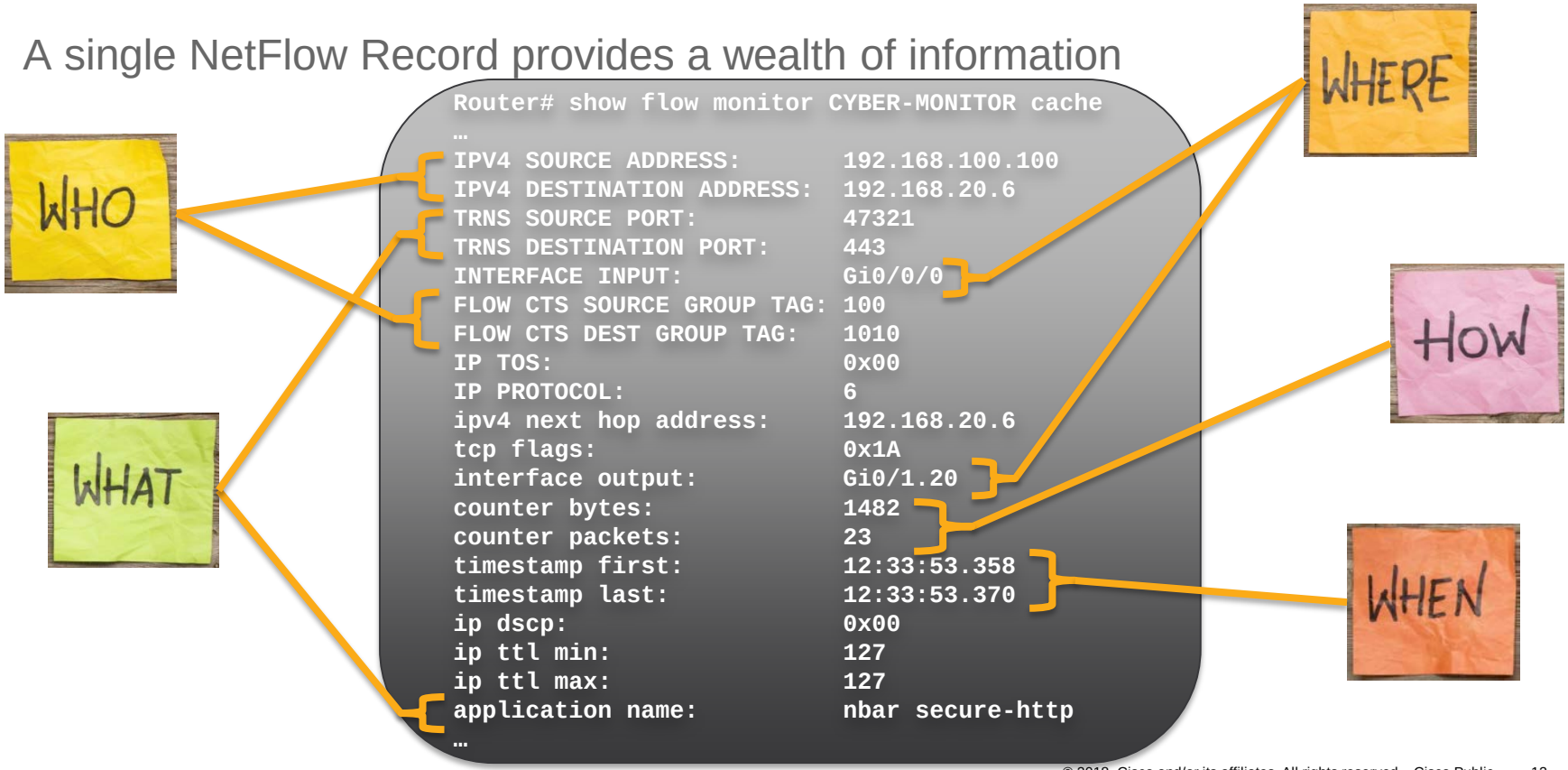
A Perfect World

- What if the entire network was a security grid?



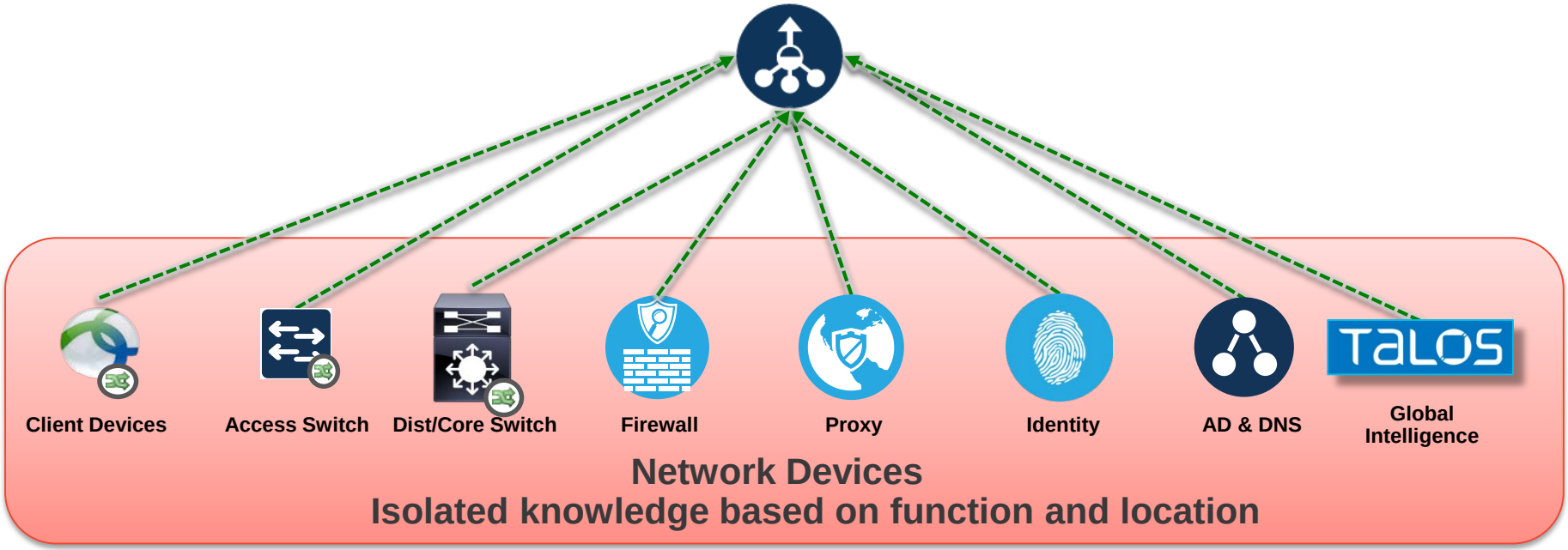
NetFlow = Visibility

- A single NetFlow Record provides a wealth of information



Complete Network Visibility

- Collect and aggregate network telemetry for the purposes of security analysis and monitoring



Thank you