cisco Engage

Data Center Innovation

Vietnam. 24-26 September 2019

Get Insights on Multi-Domain

Visibility and security in Multi-Cloud

Duc Le

ASEAN Technical Solution Architect

"93% of cloud adopters intent to be using multiple clouds in the next 12 months, and 58% of cloud adopters work with at least 4 vendors."

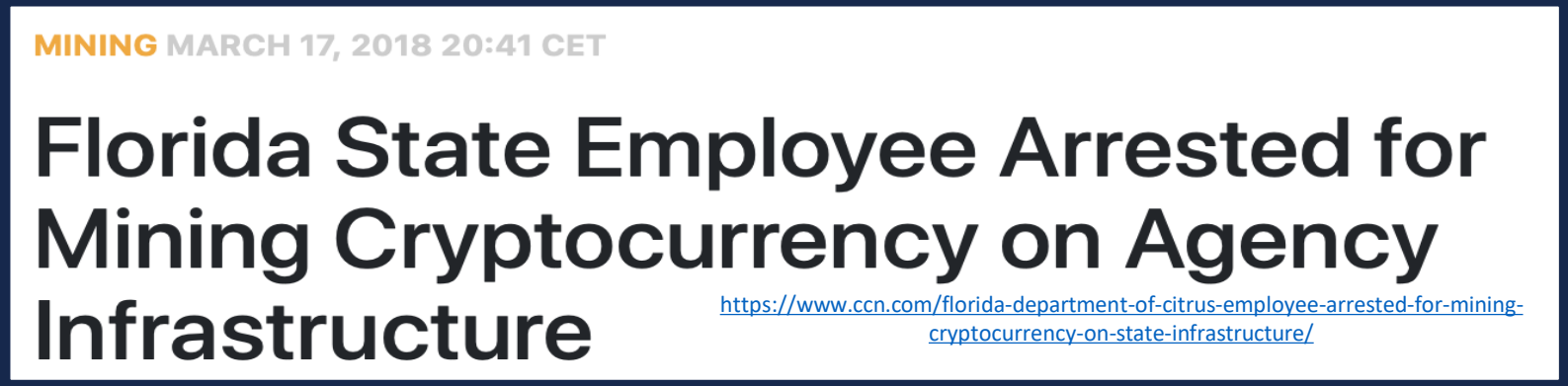
Multicloud Is the New Normal, an IDC InfoBrief, March 2018

- Cloud Workload Protection
- Lack of expertise to control the policy
- Segmentation policy.
- Vendor lock-in.
- Downtime and migration.
- Bandwidth cost.
- Operation and troubleshooting

Just another bad day in 2017-2018 …

In 2019 - Some Headlines

https://www.techrepublic.com/article/cryptomining-replaces-ransomware-as-2018s-top-cybersecurity-threat/



https://www.ccn.com/florida-department-of-citrus-employee-arrested-for-mining-cryptocurrency-on-state-infrastructure/

https://www.bbc.com/news/technology-43025788

https://www.forbes.com/sites/rachelwolfson/2018/11/13/cryptojacking-on-the-rise-webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/#a9d56afc336f

Where is it coming from?

- Attacks (BotNet, Cryptominer,…) are mainly driven by application vulnerabilities, not network ➔ network segmentation alone is not enough.
- In most cases the port will be legitimately open ➔ behavior baselining
  - Apache Struts (Port 80)
  - WannaCry (Port SMB – 139, 445)
- Attacks coming from other workloads on the same hypervisor
- Hybrid Cloud environment – How to protect your workload?
- Containers environment – scale?

Singapore Sets Cybersecurity Requirements for Banks

The Monetary Authority of Singapore, the nation's central bank, has mandated that financial institutions comply with risk management guidelines within the next 12 months in an effort to strengthen the cyber resilience of these organizations. https://www.mas.gov.sg/news/media-releases/2019/mas-issues-new-rules-to-strengthen-cyber-resilience-of-financial-industry

Key Steps

The guidelines require that financial institutions:

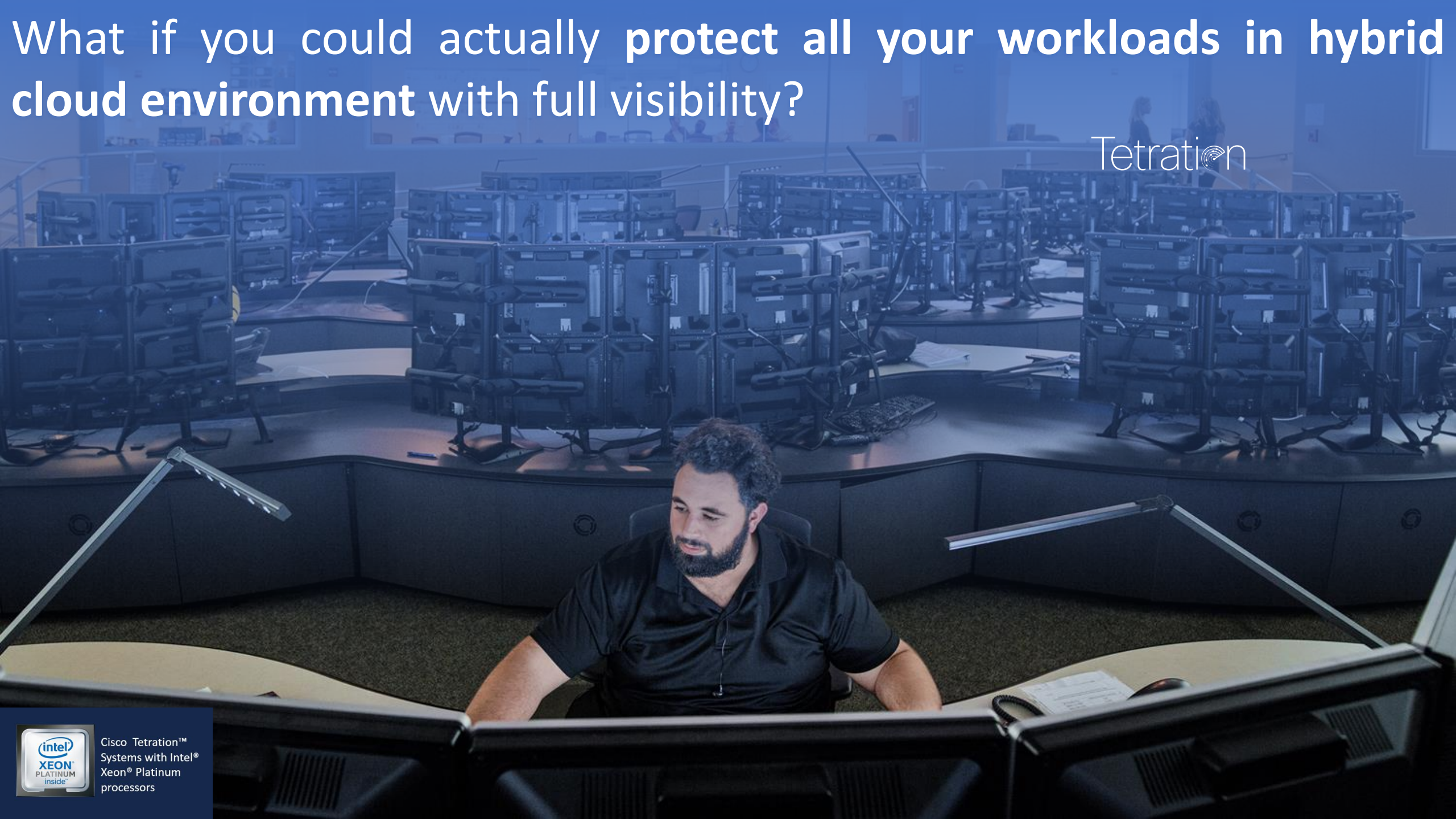
- Ensure **patching updates** are applied to address system security flaws in a timely manner;
- Deploy security devices to **restrict unauthorized network traffic**;
- Implement measures to **mitigate the risk of malware infections**;
- Secure the use of system accounts with **special privileges to prevent unauthorized access**;
- **Strengthen user authentication** for critical systems as well as systems used to access customer information.

Financial institutions have until **Aug. 6, 2020** to comply with all the new guidelines.

You make multicloud **possible**

What if you could actually **protect all your workloads in hybrid cloud environment** with full visibility?

Tetration



Holistic Approach to protect your workloads

PROTECTION

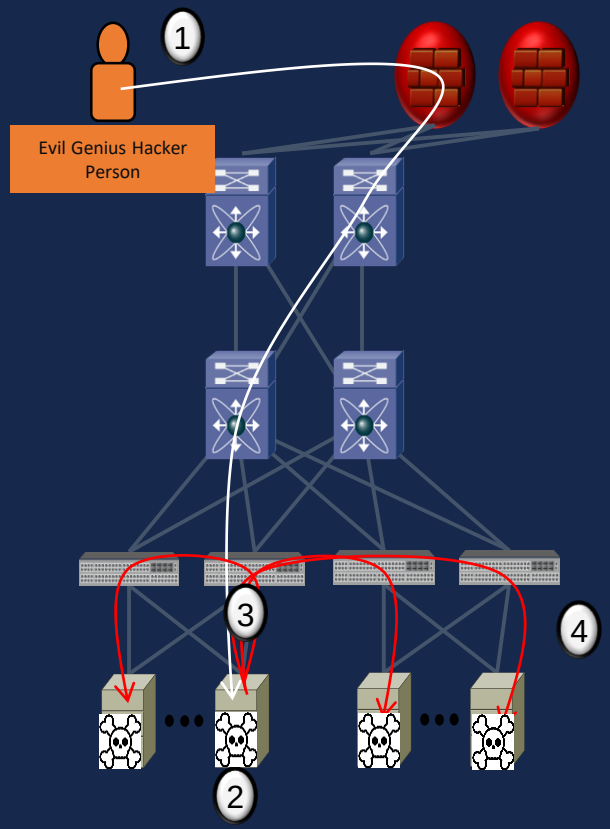
PREVENTION

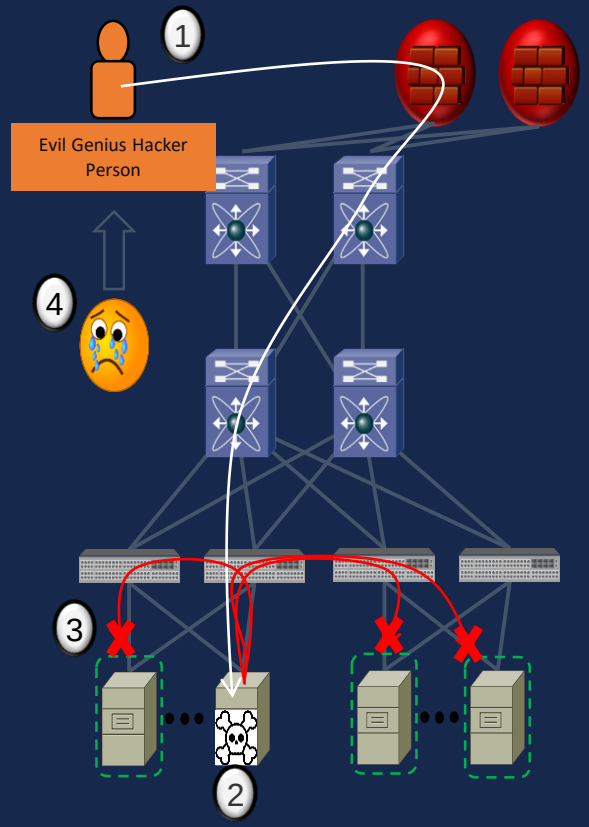
DETECTION

REACTION

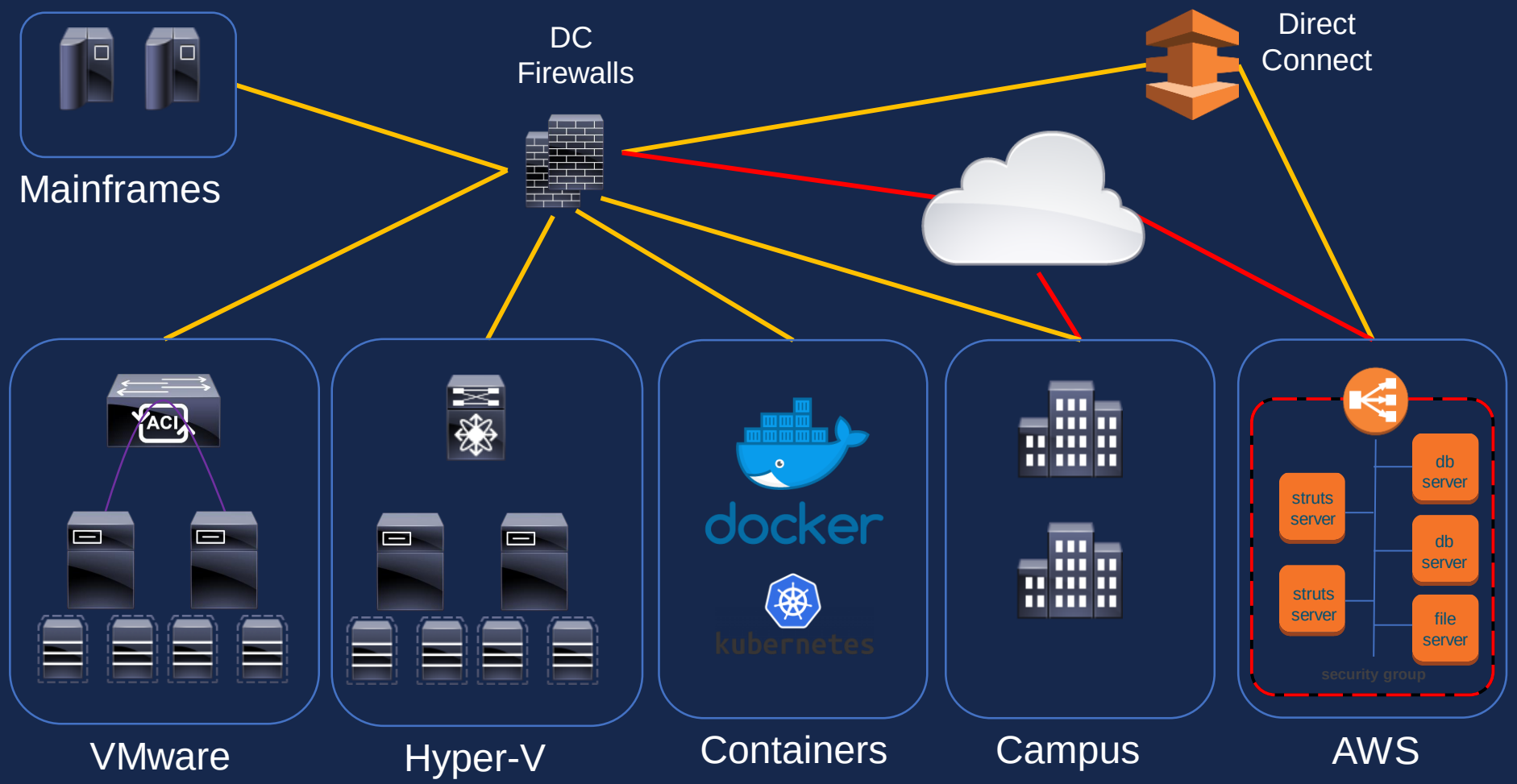
make multicloud possible

Purpose of segmentation



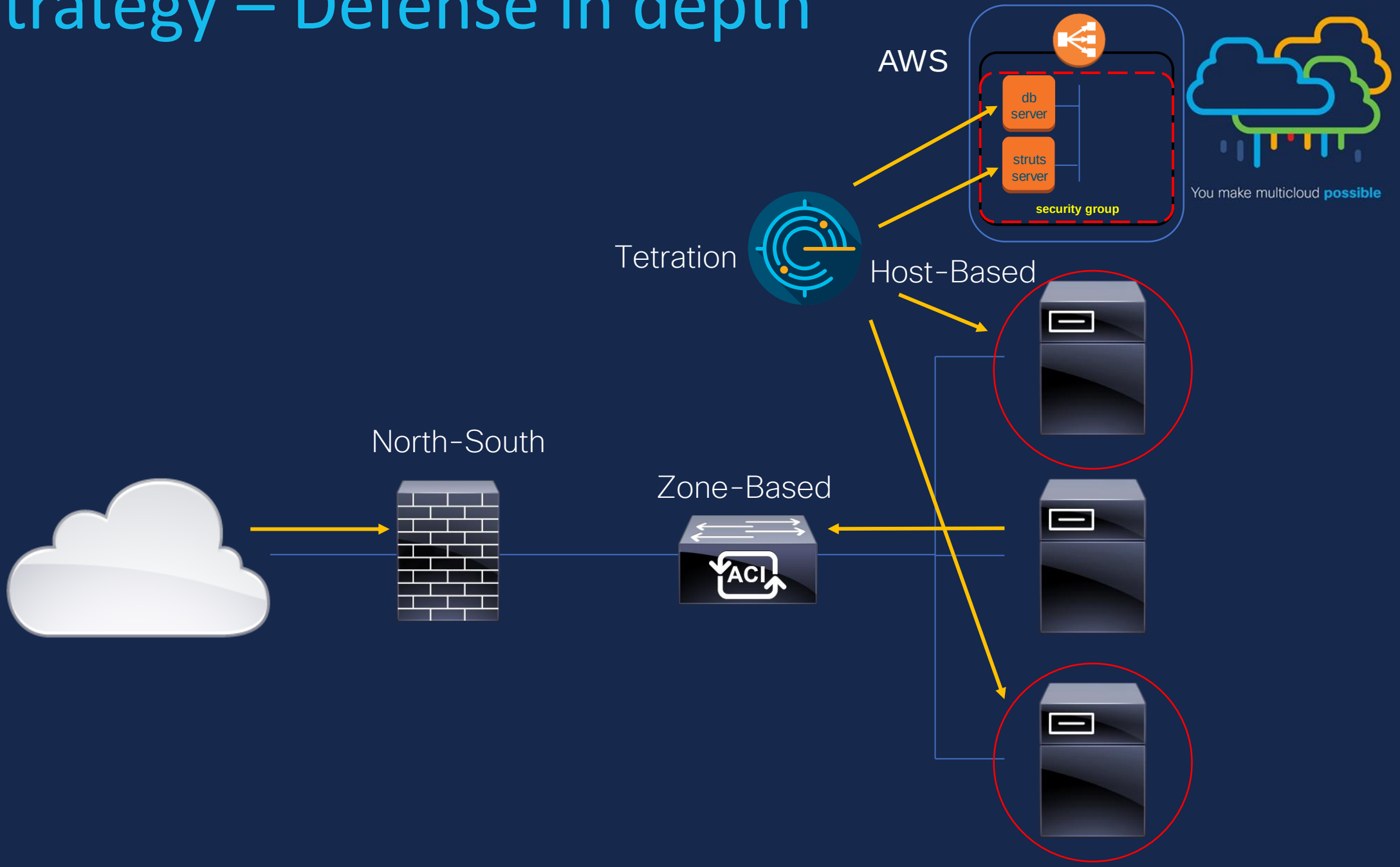


Segmentation your network



You make multicloud **possible**

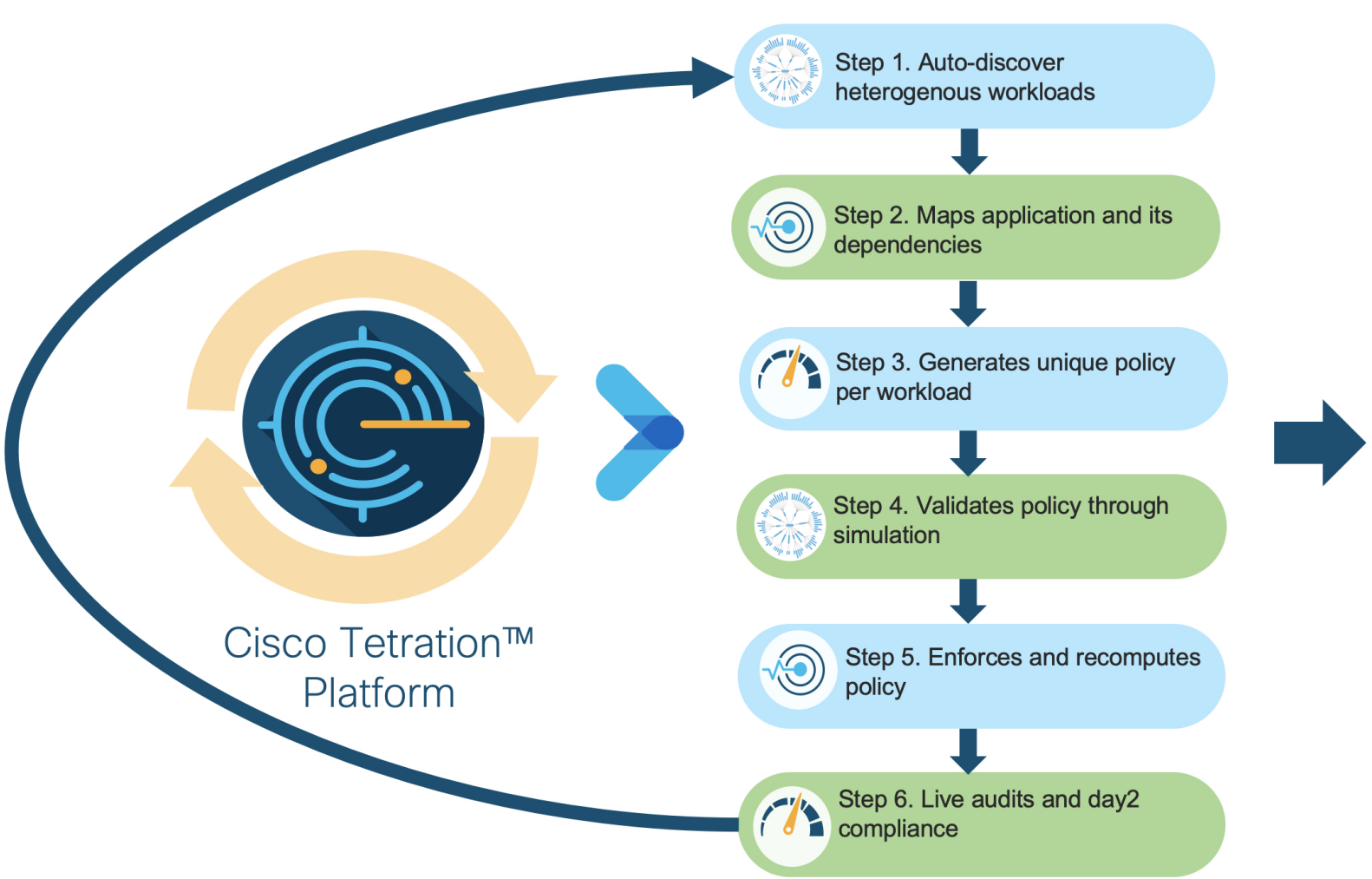
The Strategy – Defense in depth



Tetration, Segmentation Made Easy

Cisco Tetration™ with Intel® Xeon® Platinum processor

Full-Lifecycle policy Discovery, Management and Enforcement



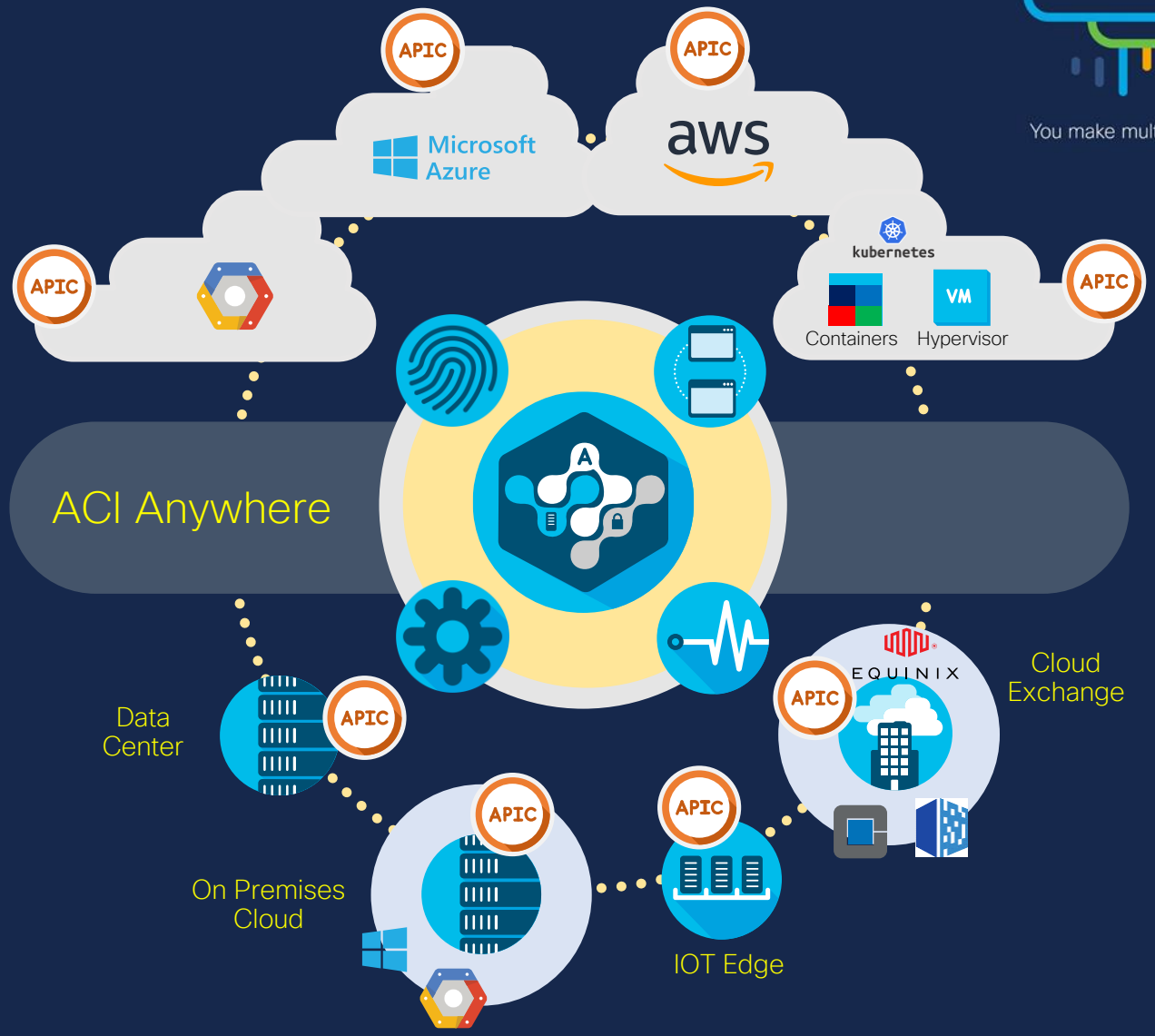
80% Reduction in Attack Surface

90% Faster Time to Value

85+% Reduction in Security Rules

ACI Anywhere

- Operational Simplicity: Same “look and feel” as On-Premise
- Automated Policy Translation: Consistency across the entire data center
- Common Governance: End-to-end discovery, visibility and troubleshooting



You make multicloud **possible**

Singapore Sets Cybersecurity Requirements for Banks

The Monetary Authority of Singapore, the nation's central bank, has mandated that financial institutions comply with risk management guidelines within the next 12 months in an effort to strengthen the cyber resilience of these organizations. https://www.mas.gov.sg/news/media-releases/2019/mas-issues-new-rules-to-strengthen-cyber-resilience-of-financial-industry

Key Steps

The guidelines require that financial institutions:

- Ensure patching updates are applied to address system security flaws in a timely manner. **Tetration: Vulnerability Discover.**
- Deploy security devices to restrict unauthorized network traffic. **Tetration: Every traffic, every flow at line rate, to build whitelist policy automatically.**
- Implement measures to mitigate the risk of malware infections. **Tetration: Threat Detection and remediation process using whitelist policy.**
- Secure the use of system accounts with special privileges to prevent unauthorized access. **Tetration: Detect privileges escalation in every workloads.**
- Strengthen user authentication for critical systems as well as systems used to access customer information. **Tetration: integrate with ISE/NAC and work with DUO for Zero-Trust and policy enforcement for end-user.**

Financial institutions have until Aug. 6, 2020 to comply with all the new guidelines.

You make multicloud **possible**

Specifically for Multi cloud, *you can*…

You make multicloud **possible**

- Dynamically learn **application dependency mapping** for **cloud migration**
- Dynamically generate updated and **real-time whitelist policy** for hybrid cloud environment
- **Analyze** information about hybrid cloud workloads and gain **pervasive visibility**
- Classify them to your enterprise security policy **intent**
- **Enforce *same* security policy** for workloads in the public cloud as you do within your enterprise – **cloud agnostic**
- **Test** the **policy** and **cloud migration scenarios** to see the **cost and impact**
- Build **security dashboard** for your hybrid cloud environment to understand the **security position**
- **Detect** when you get **attack** in your multi-cloud environment

KEEP CALM IT IS DEMO TIME

cisco Engage

Data Center Innovation

Vietnam. 24-26 September 2019