illumio

Zero Trust

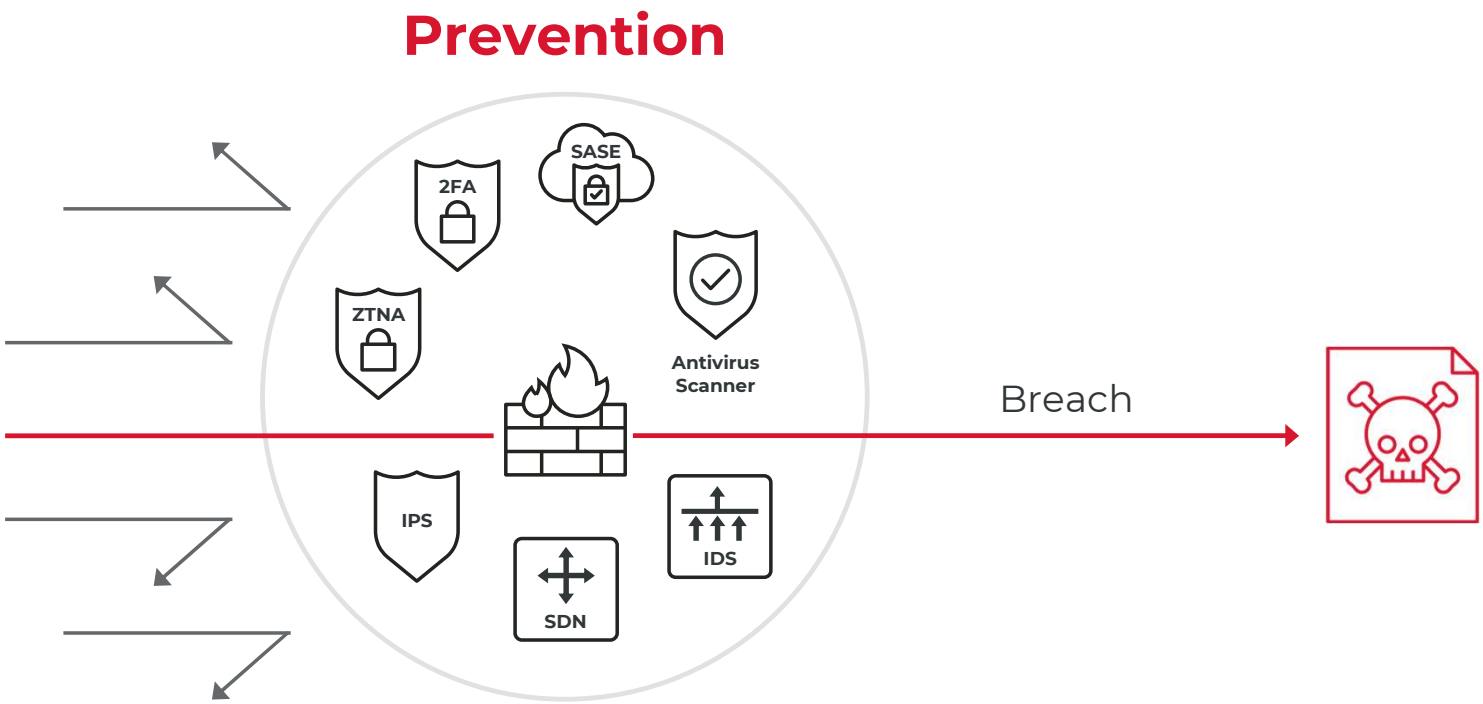
Independent of Network Security

Protect against un-detected threats

Christer Swartz
Director, Industry Solutions

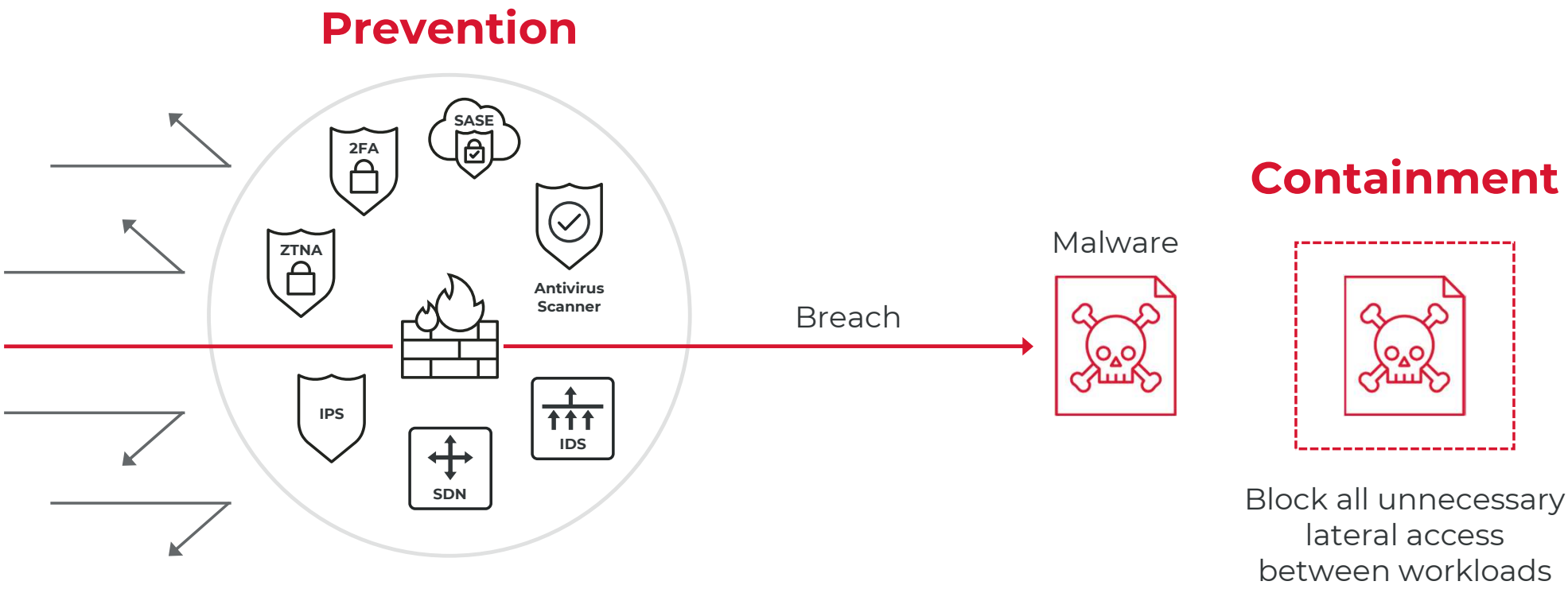
Reality Check: You will be breached

No Prevention solution is 100% effective. *Surviving* a breach needs to be equal priority.

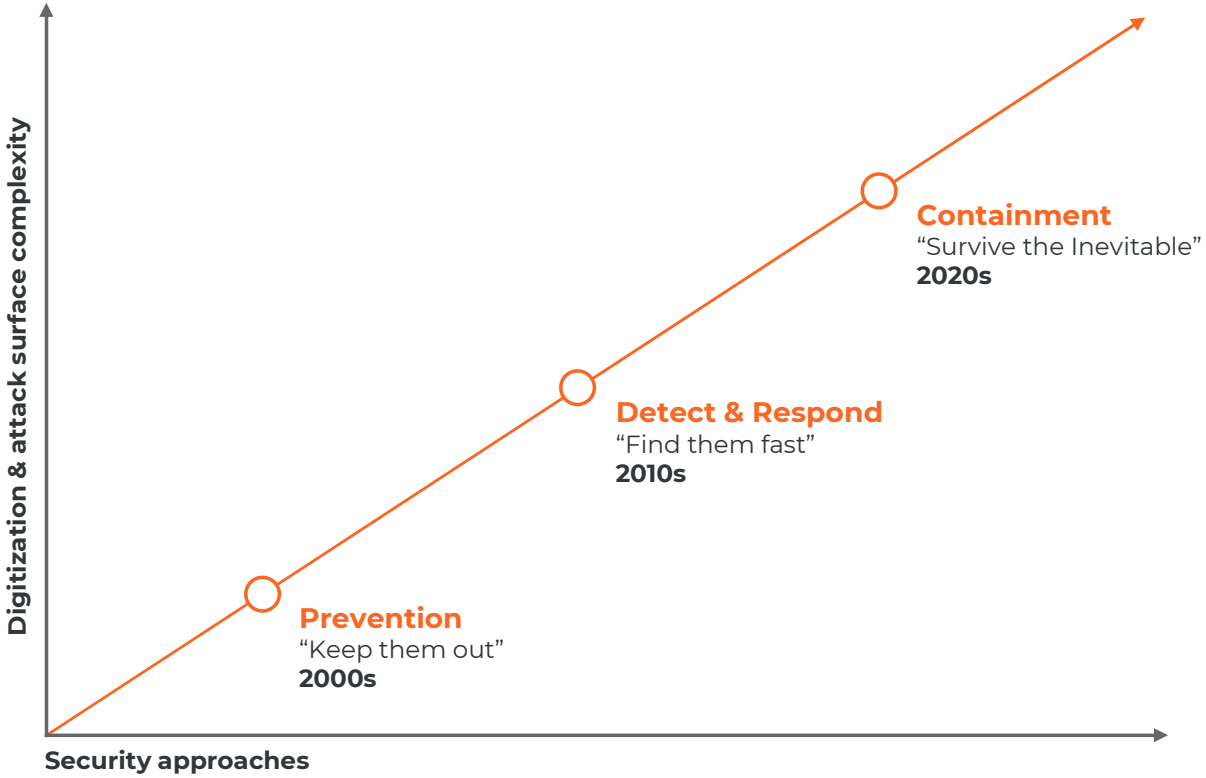


Is it possible to protect against un-detected threats?

Contain *unknown* threats by preventing the methods used to spread.



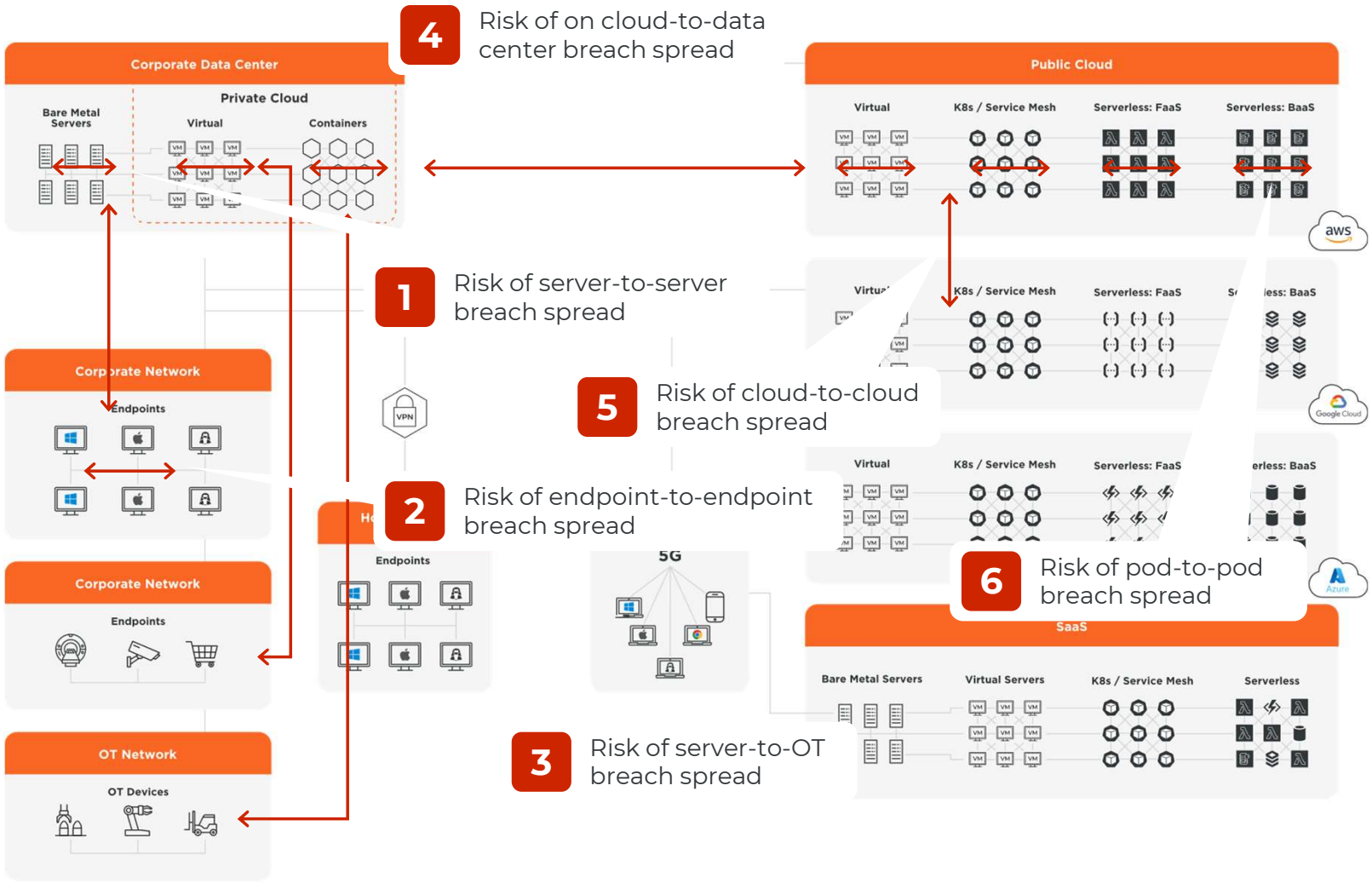
Breach containment is the new paradigm



illumio

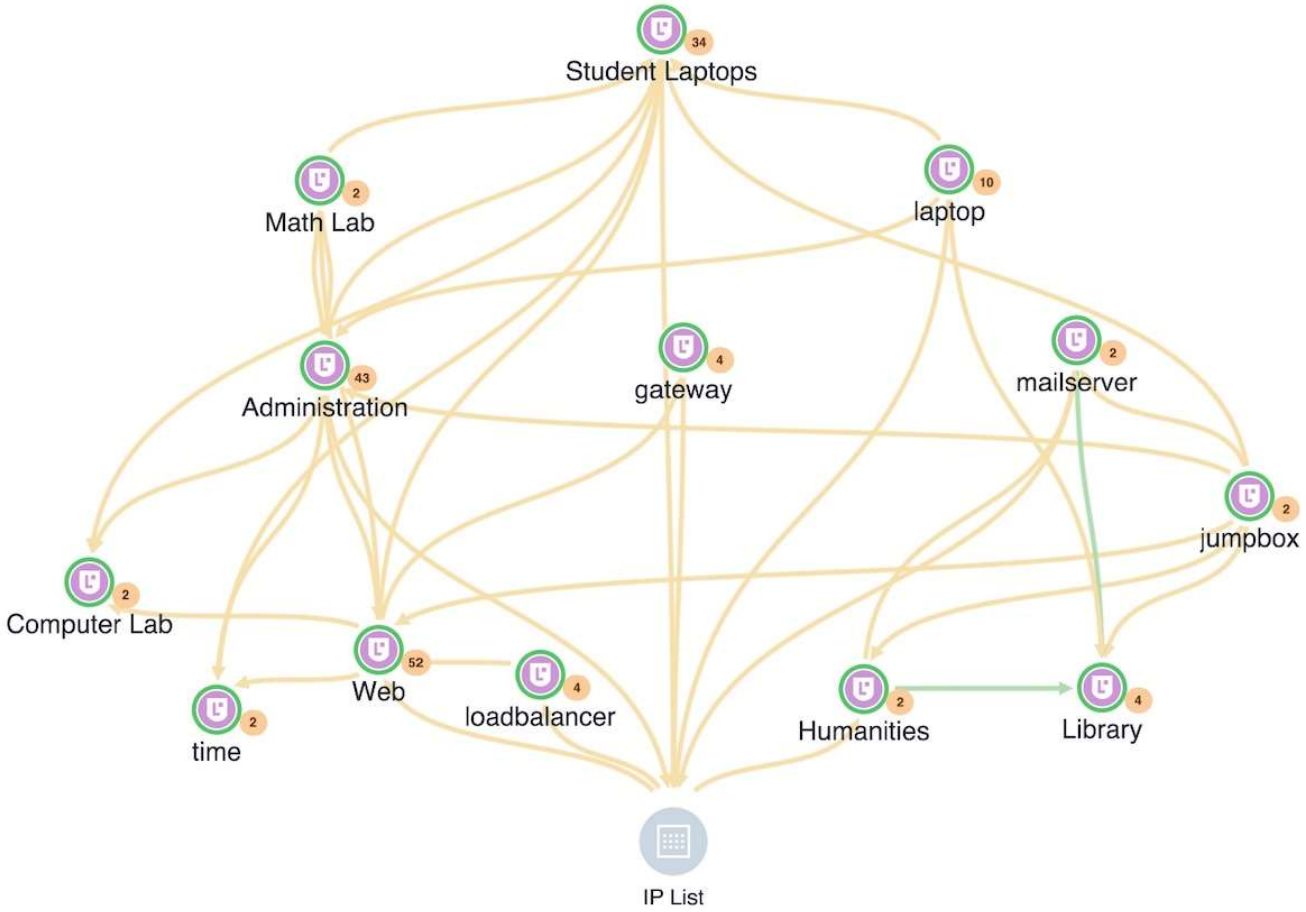
Most threats share 1 thing in common: they want to spread

Threat actors have many entry points to choose from.

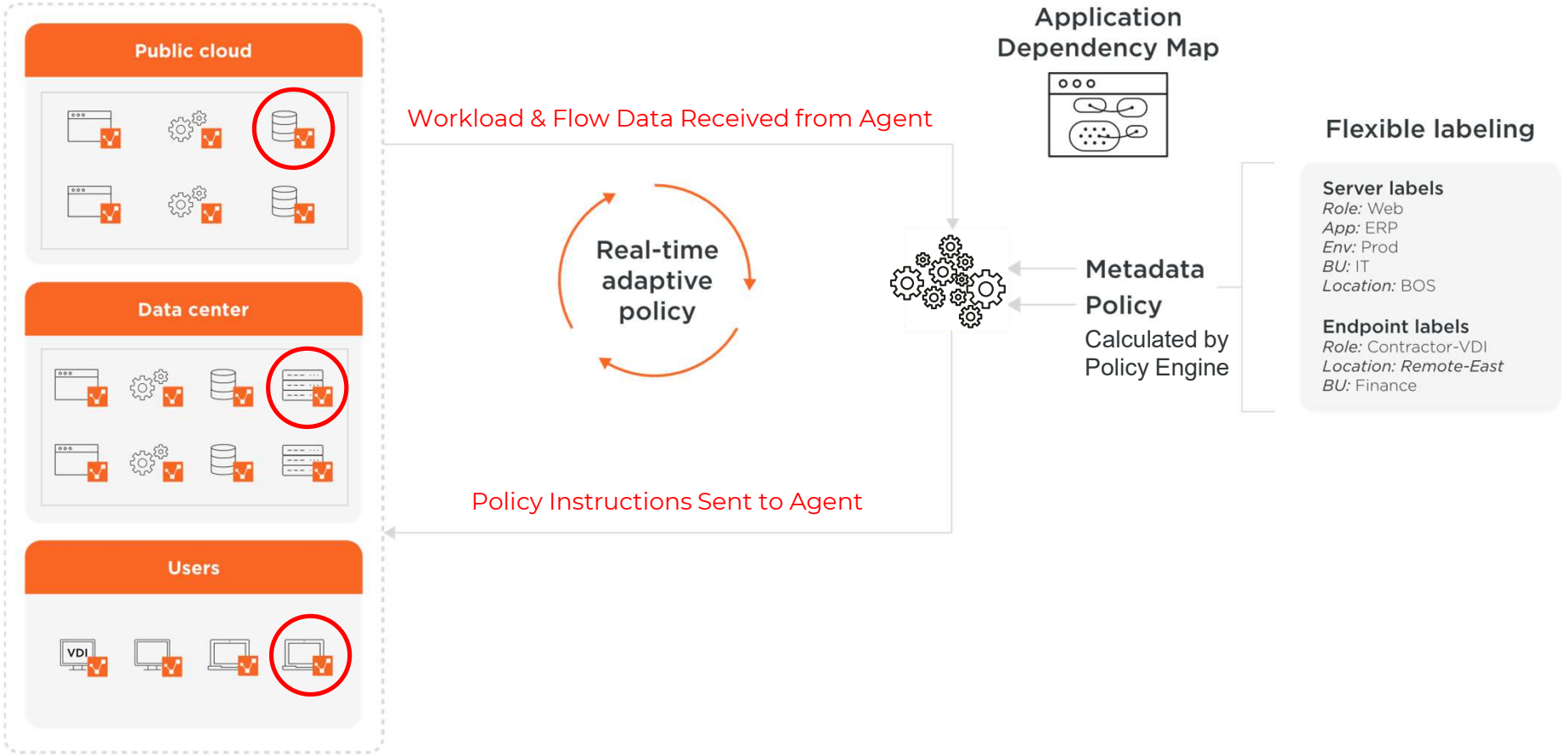


illumio

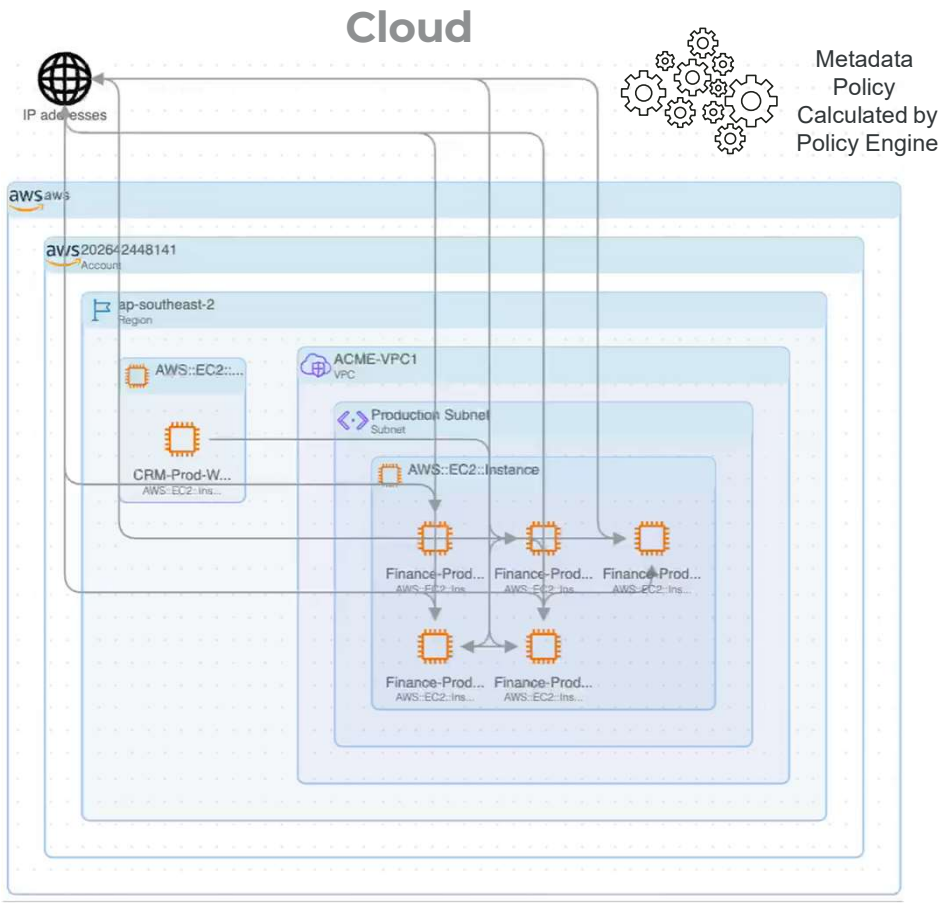
First Step: Visibility, Showing All Application Dependencies

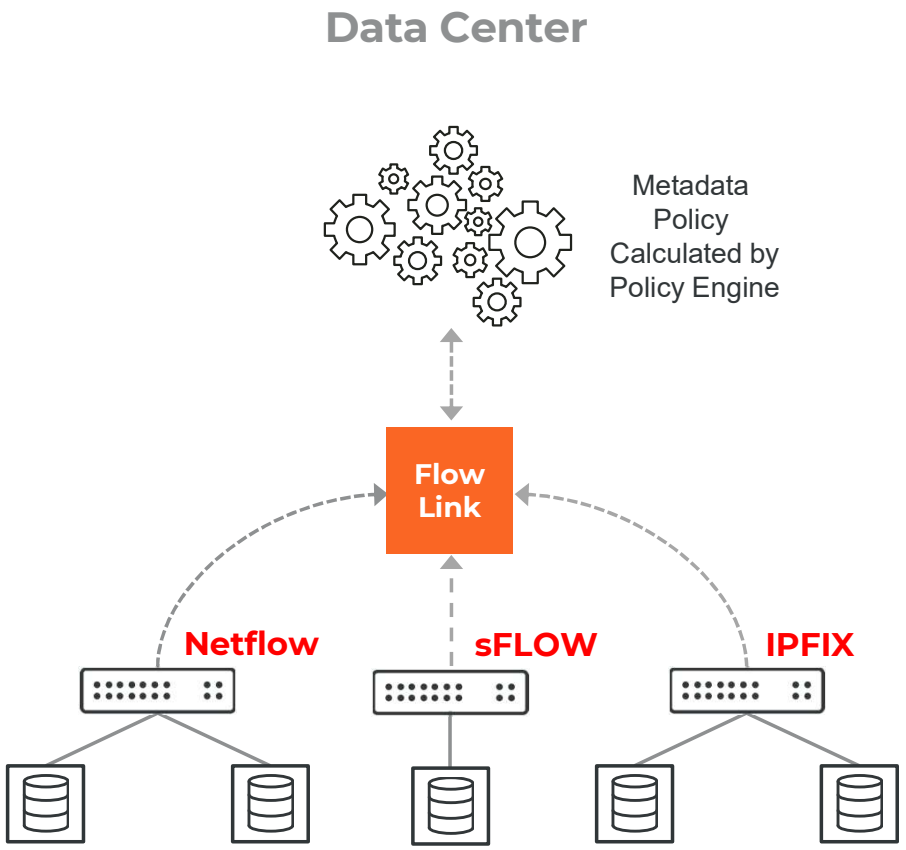


Agent-Based Visibility & Enforcement: Directly at Workload

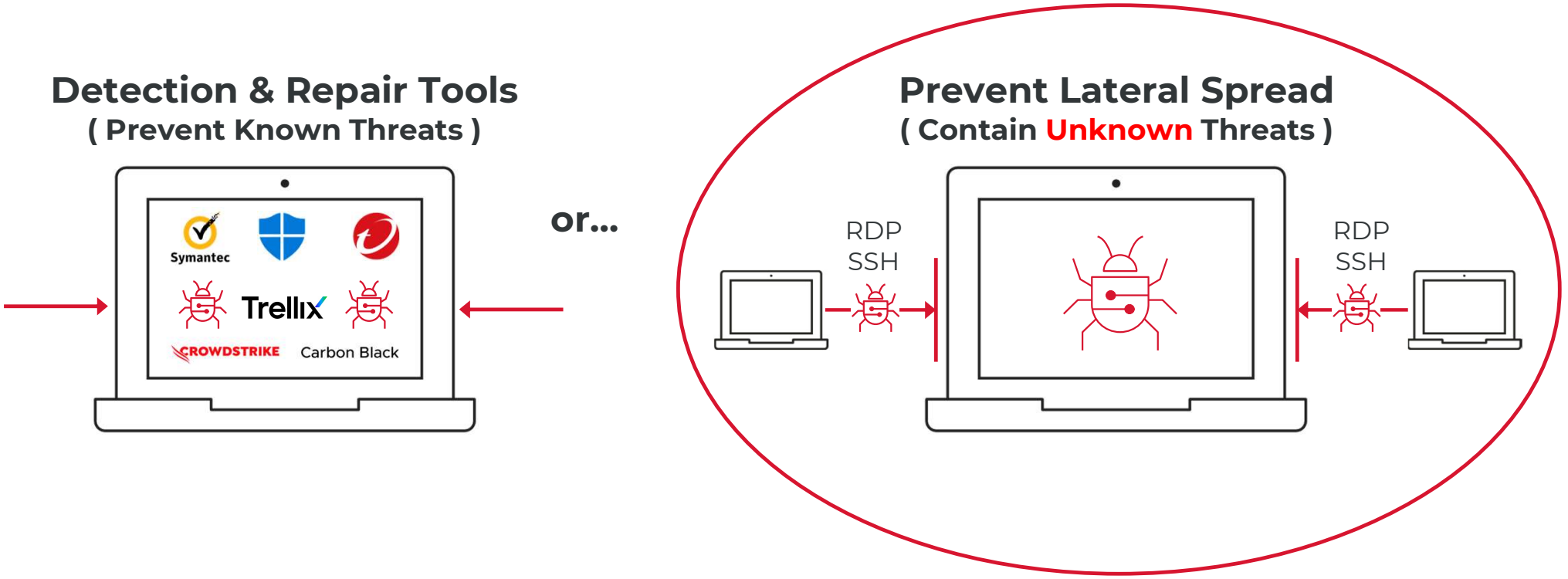


Agentless Visibility & Enforcement: In the underlying Fabric





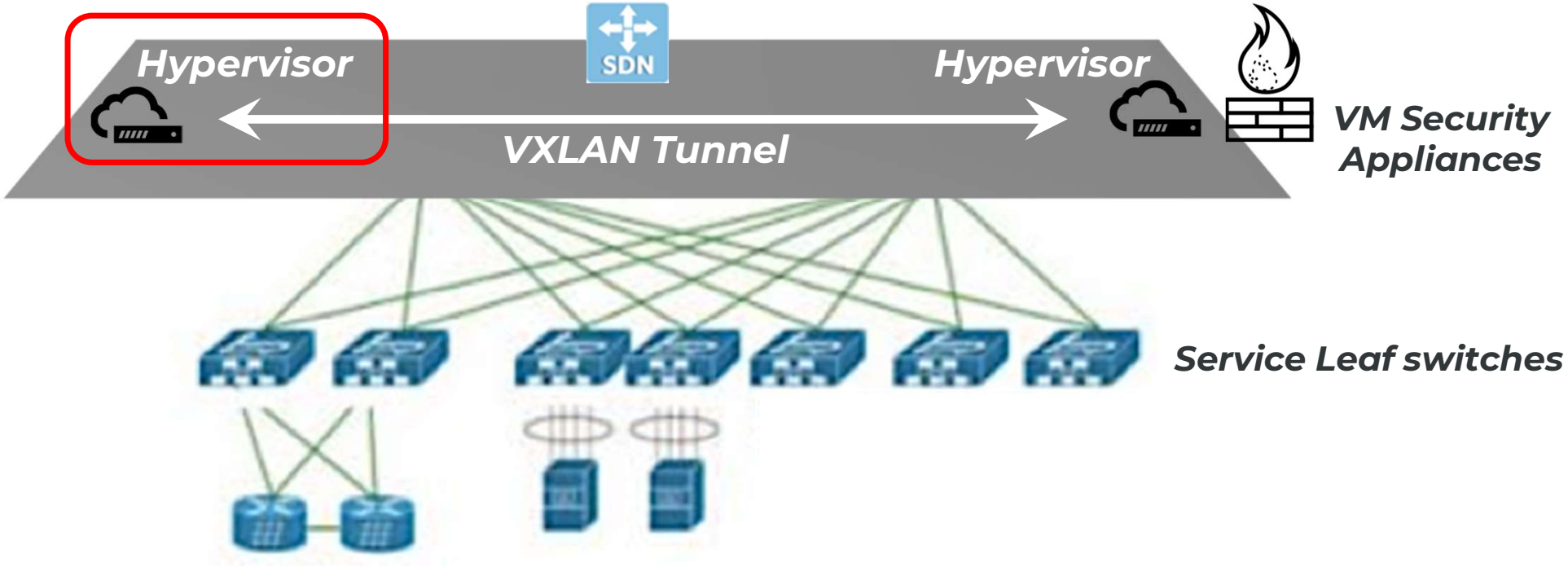
Keep resource healthy, or sacrifice to stop lateral spread?



Private Cloud: Example, NSX SDN Overlay Networks

- Many Private Cloud platforms are **hypervisor-centric**, with the hypervisor as the virtualized network edge. This is challenging when adding Public Cloud to Private Cloud architecture: there are no hypervisors accessible in Cloud. **Security model becomes silo'd**.

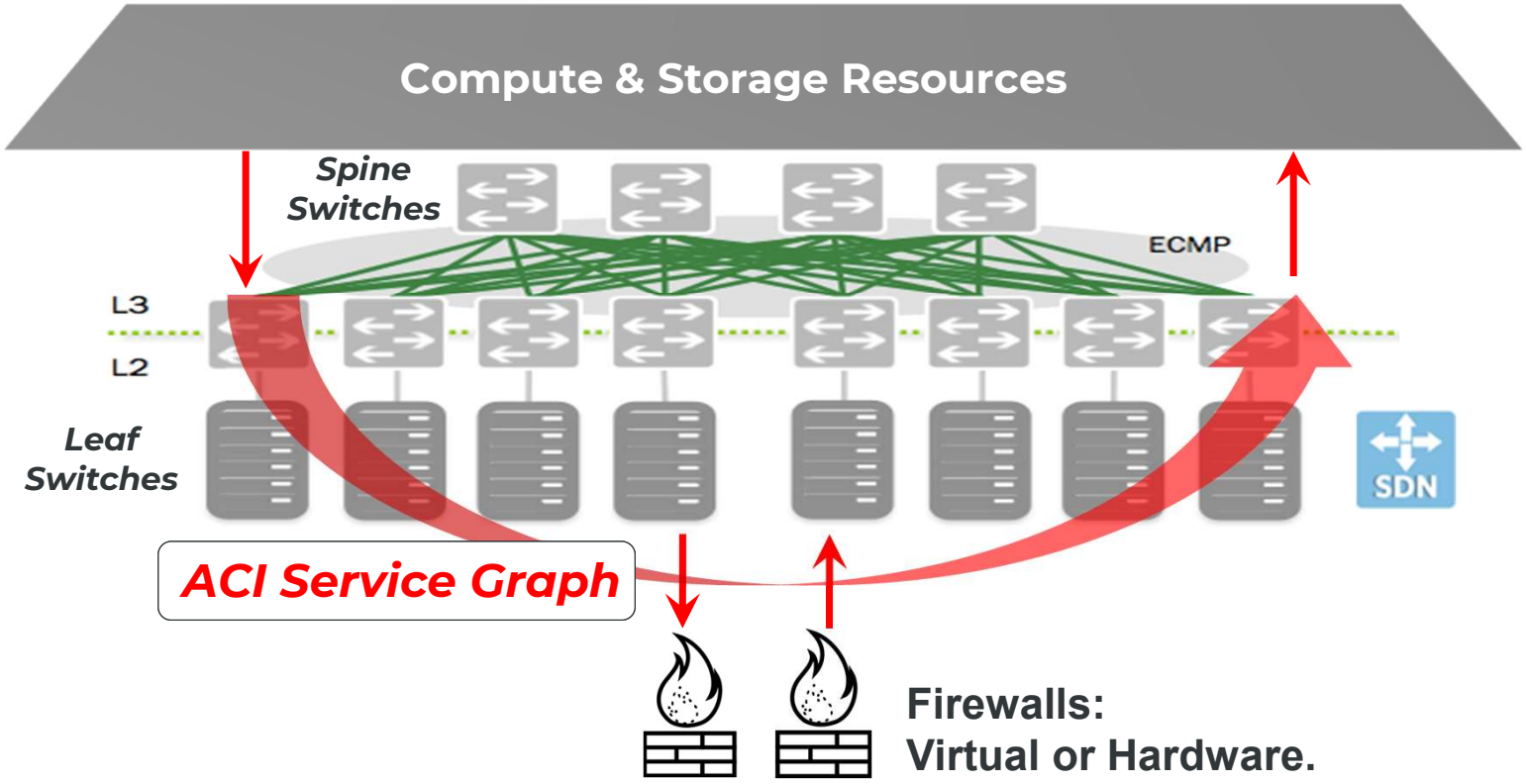
- Extending NSX into Cloud requires deploying bare-metal servers in Cloud Data Centers, and deploying hypervisors there. The result is Cloud silos and significant security complexity.



Private Cloud: Example, Cisco ACI SDN Tunnel Re-Directs

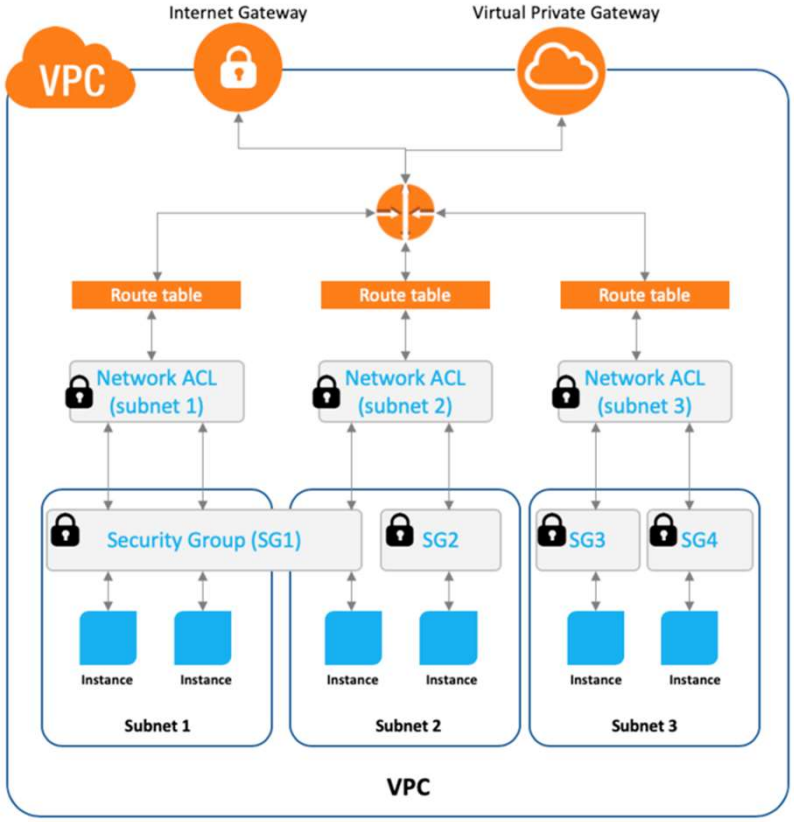
- Cisco ACI re-directs VXLAN tunnels to Firewalls deployed in Service Leaf switches. This makes ACI largely Data Center **hardware-dependent**. Segments are EPG's: **complex at scale**.

- Extending ACI into Public Cloud requires extending virtualized network topology on top of Public Cloud topology, maintaining a network-centric security model, and quickly becomes very operationally complex.

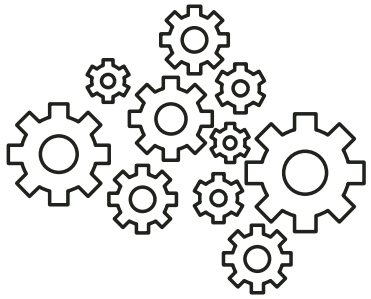


Public Cloud: Security Groups, NSG's, Virtual Appliances

- Security Controls in Cloud are mostly network-centric, just virtualized.
- Each Cloud vendor's security tools are different from each other.
- Cloud metadata needs to be mapped to Application-centric security Policy model, operationally consistent across Clouds.



What is the minimal amount of information required to block malware?

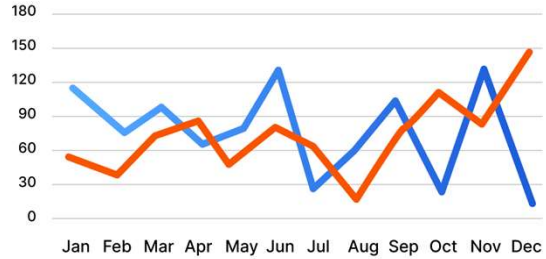


Collect lots of complex Layer-7, Behavioral Analytics information, copy packets, & do deep analysis?

Or Collect “just enough” information to block propagation?

Deep Intelligence = Time is lost before making a decision

Prevent lateral spread before spending time understanding the nature of the threat.



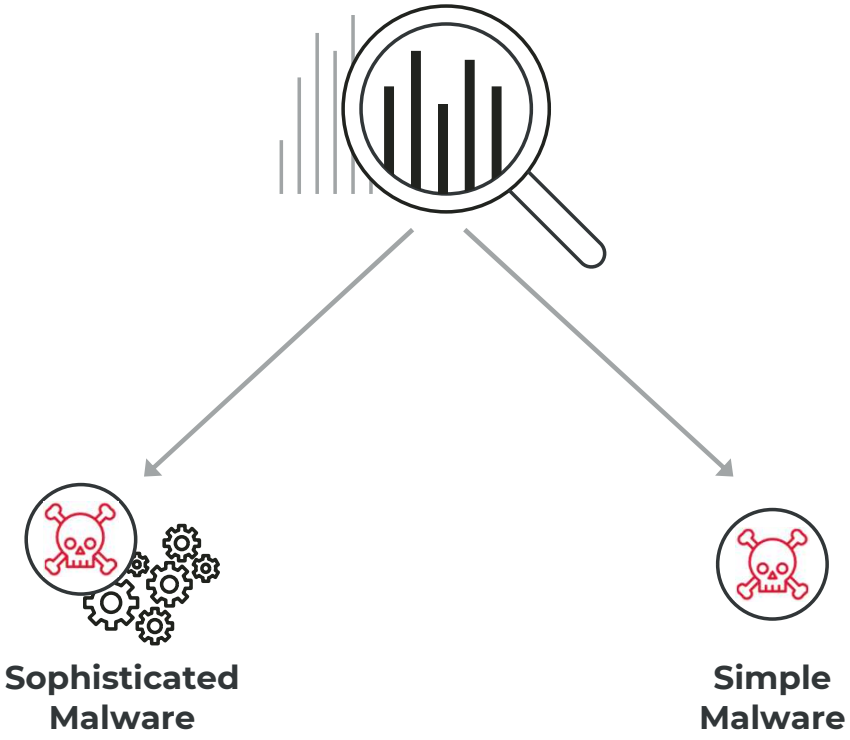
Deep intelligence,

Complex solution to a simple problem

Data Center | **Public Cloud** | **Mobile Users**

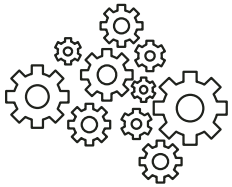
After blocking then threat, then it's time to dig deeper

Digital Forensics
AI / ML / DPI / L7 Intelligence



Automate the tools you already have: OS firewalls

Centrally orchestrate the ability of all modern OS's to enforce traffic directly at workload.



Linux
iptables & nftables

Windows
Windows Firewall

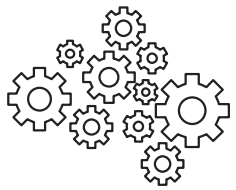
Containers
iptables

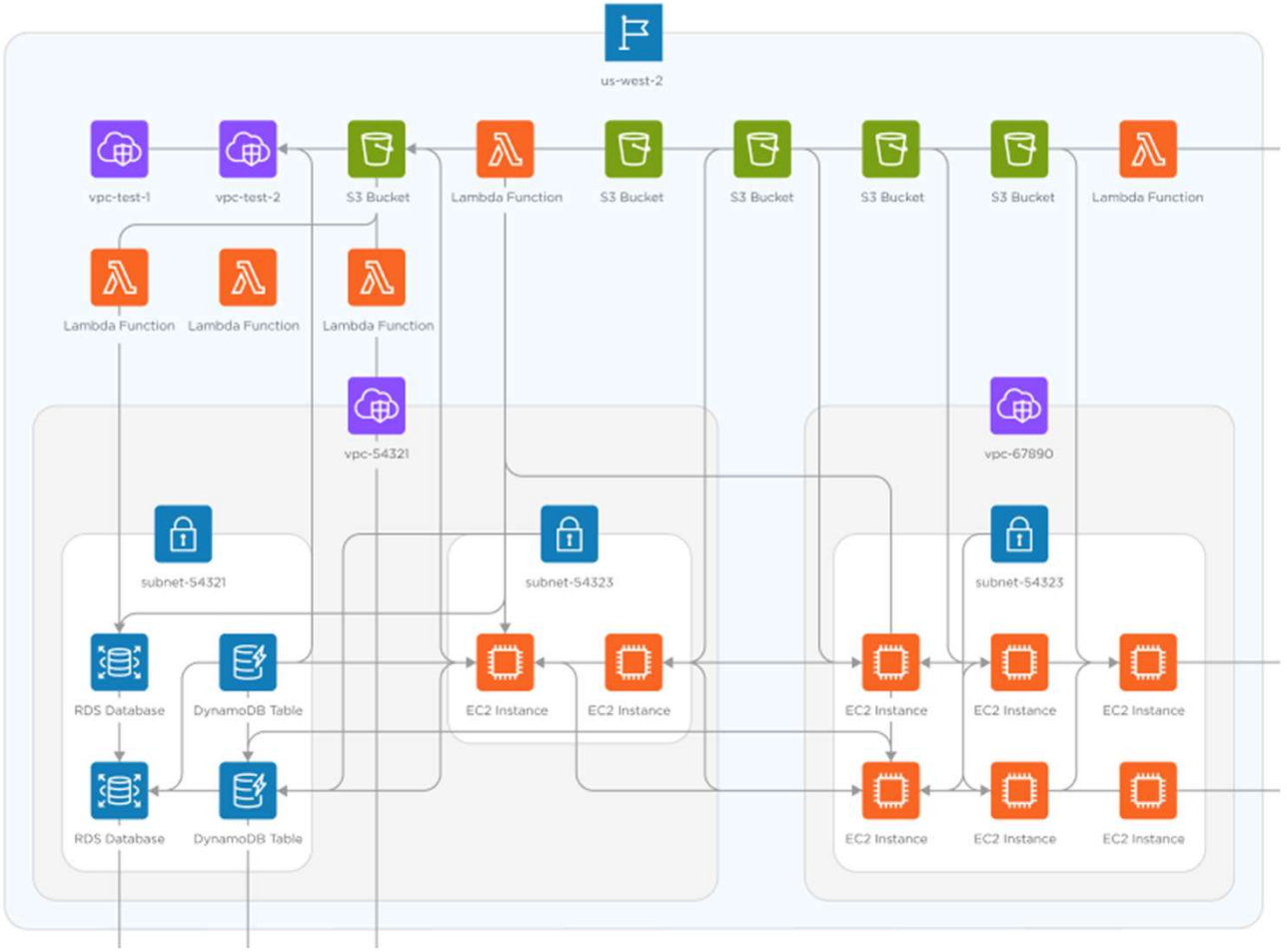
MacOS
Application Firewall (ALF)

IBM
Filter Rules

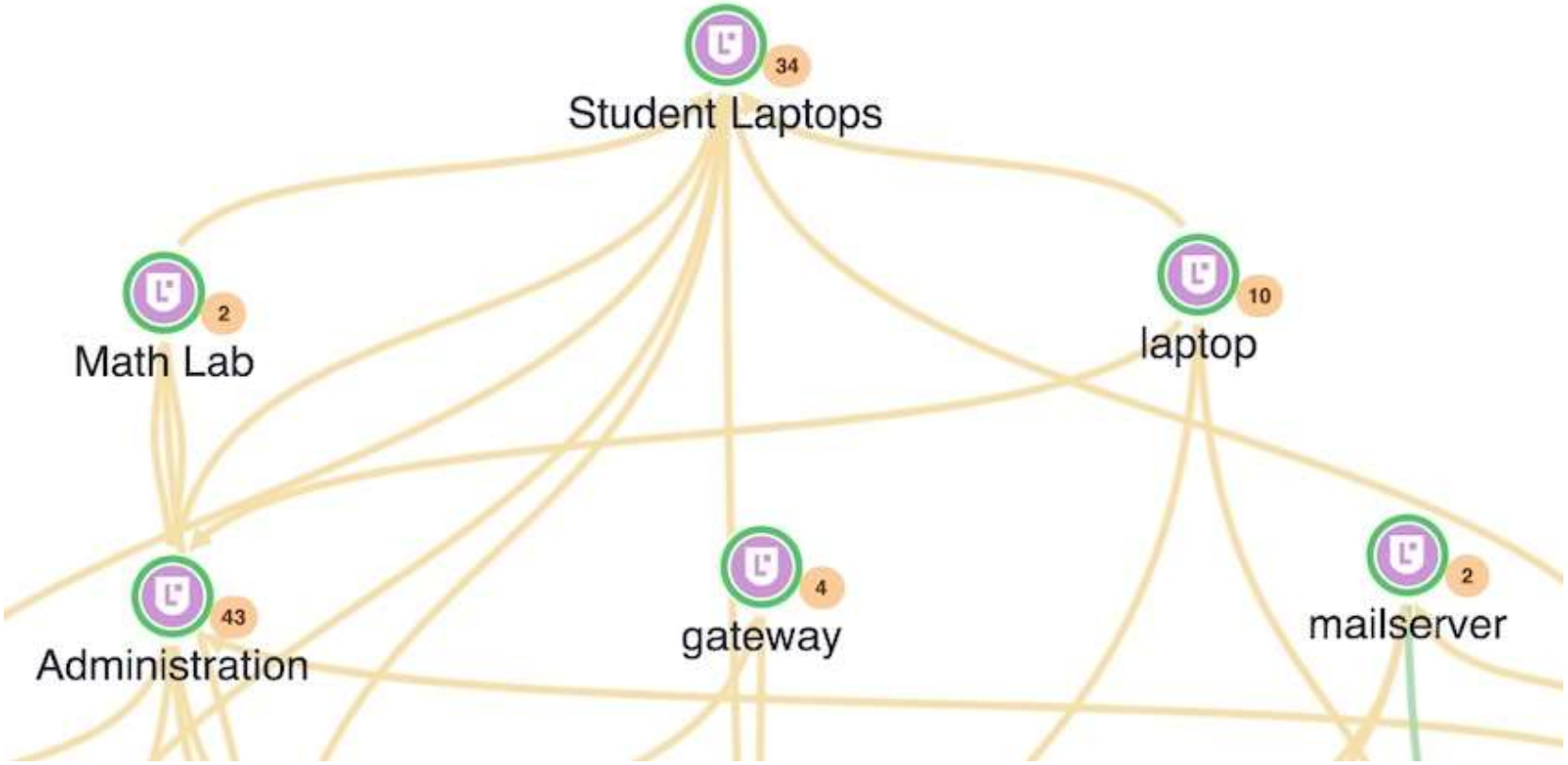
Oracle
Packet Filter

Automate Harvesting of Metadata & Workloads from Cloud





Metadata: Human-Readable Labels

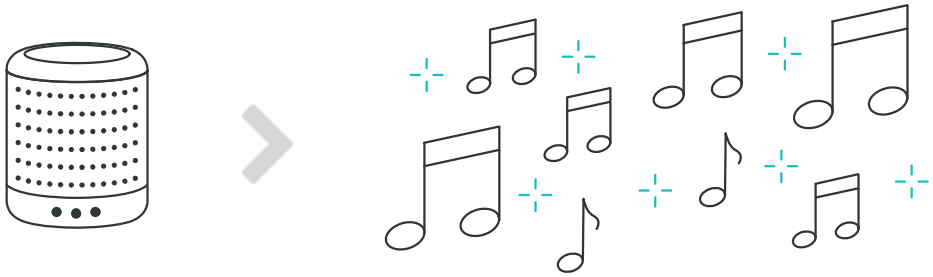


A Declarative Model: Define the “What”, not the “How”

Don’t worry about Policy rule-order.

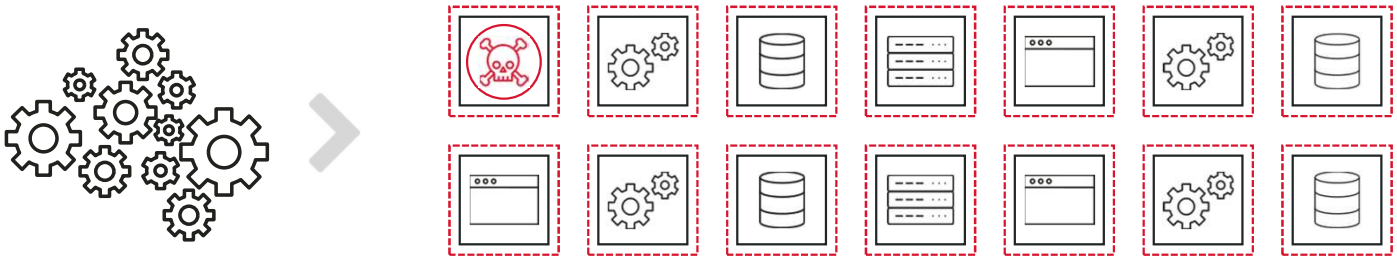
Hey Alexa:

“Play music”

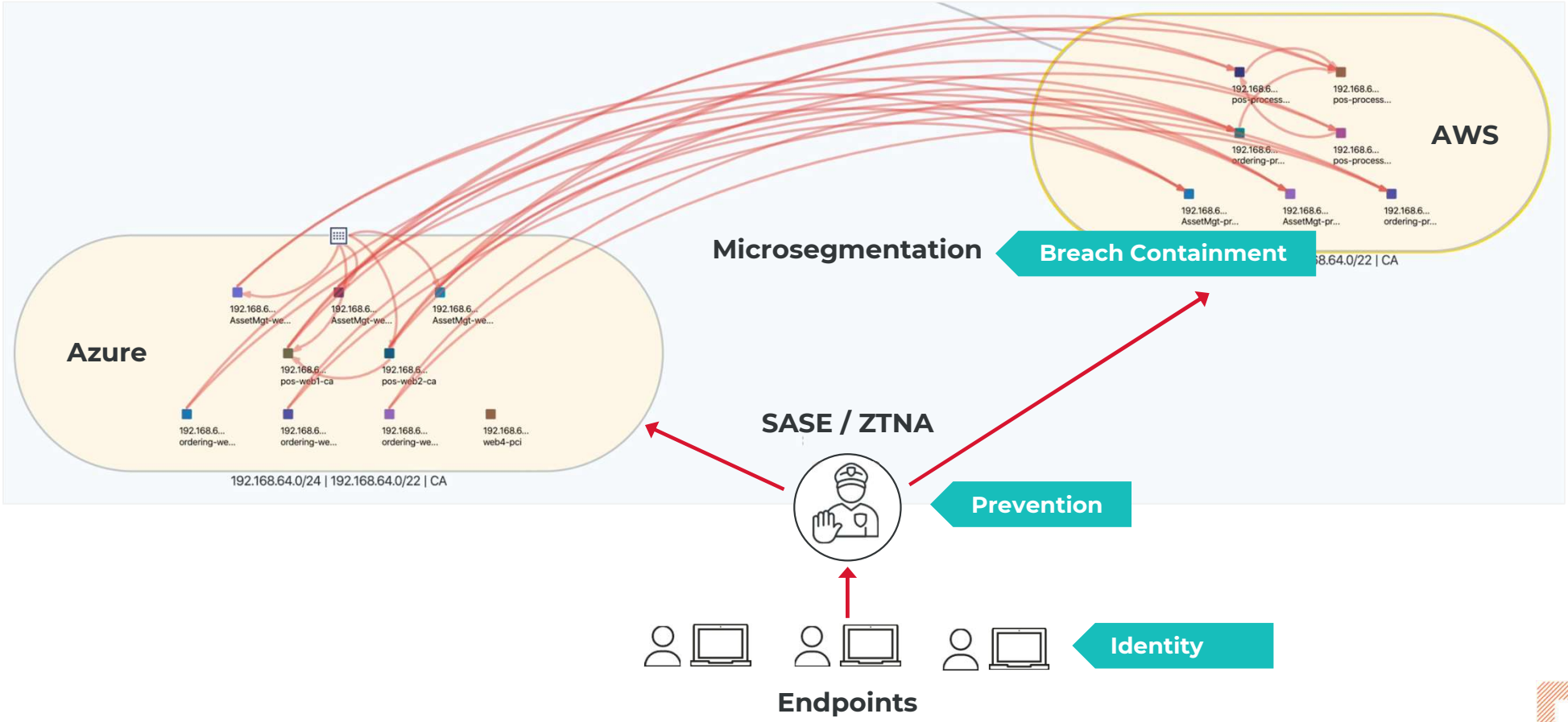


Hey Segmentation Engine:

“Block RDP & SMB ports for all Workloads labeled as Database, in Production, in London”

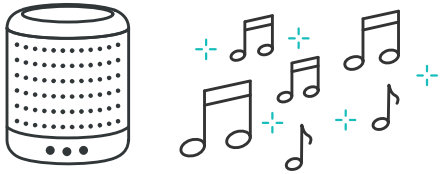


The 3 Zero Trust Remote Access Enforcement Points



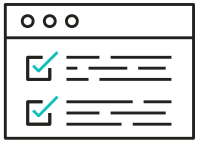
Benefits of the Breach-Containment Security Model

Small problems don't escalate into big problems



A Declarative model: Define the "What", Engine does the "How"

Quickly block Command + Control traffic. *Protect against un-detected threats.*



Test/Simulate before deploying Policy. No more "deploy-and-pray"

Sleep well, knowing your company won't appear in the news tomorrow

Stay Tuned: AI-Generated Malware

Malware created by Generative AI will still want to spread. Block the pathways now.