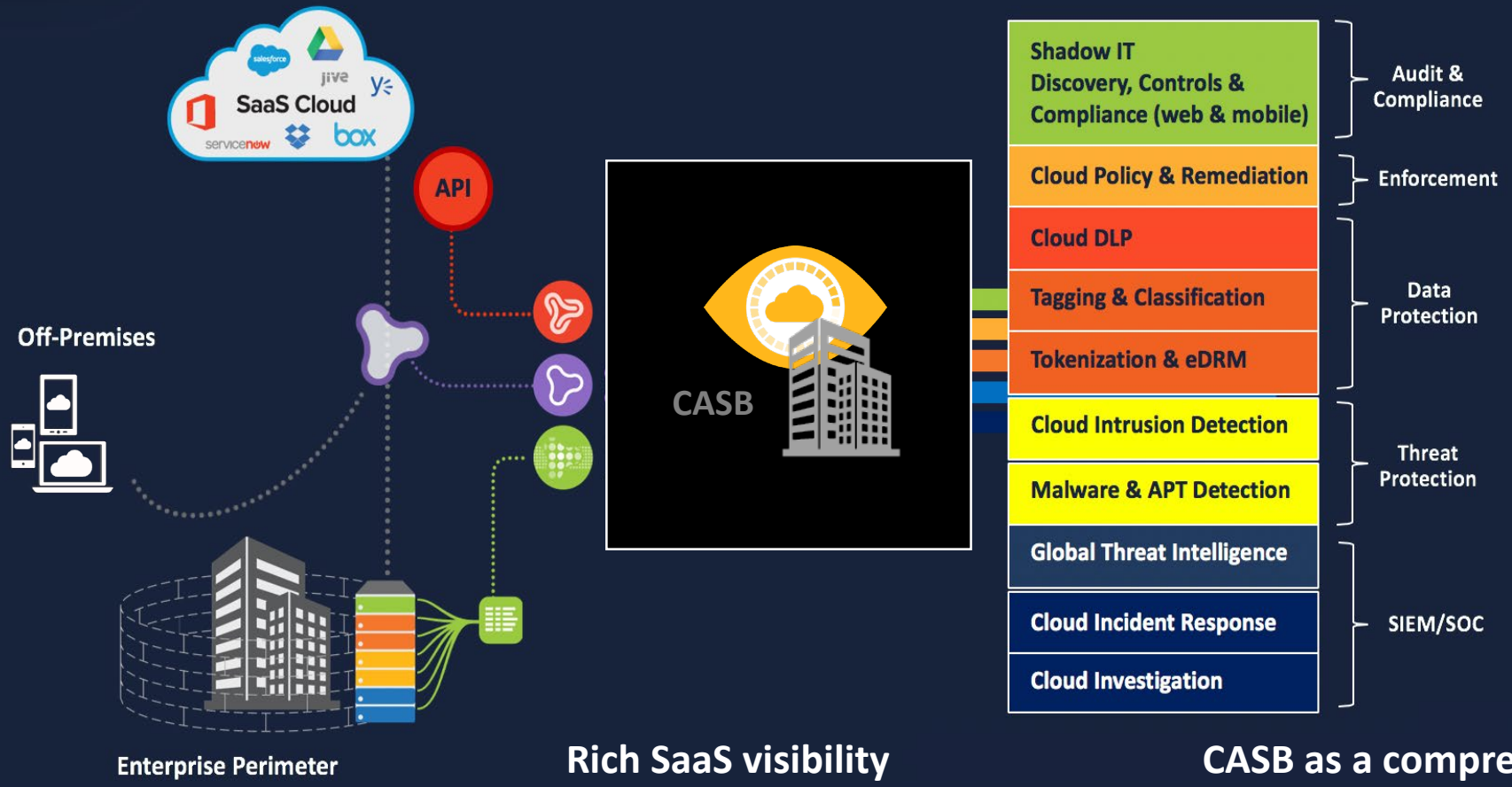
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO3-T08

How to Apply a Zero-Trust Model to Cloud, Data and Identity

Nico Popp
Sr. VP of Information Protection
Symantec

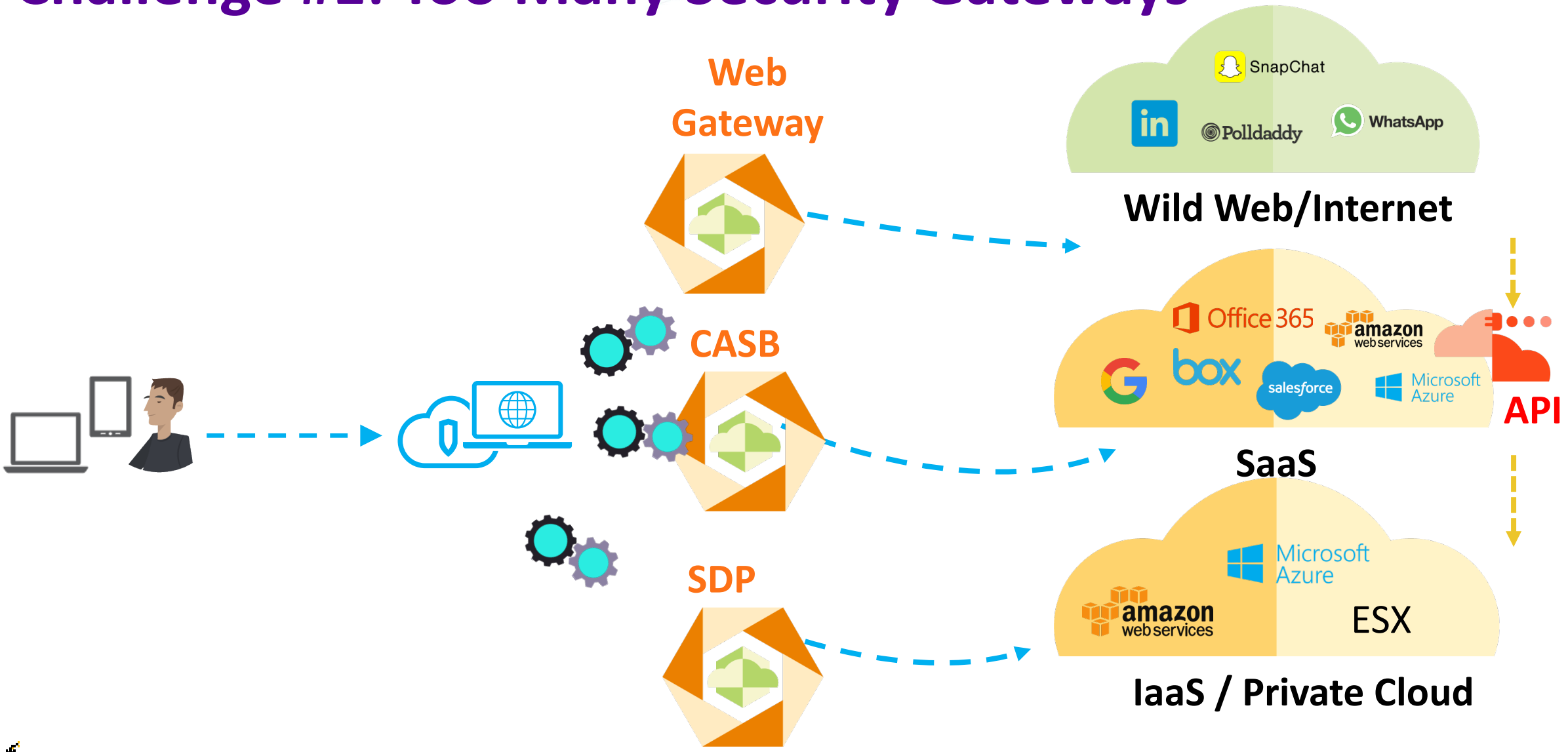
Cloud Security Status Quo Today: CASB



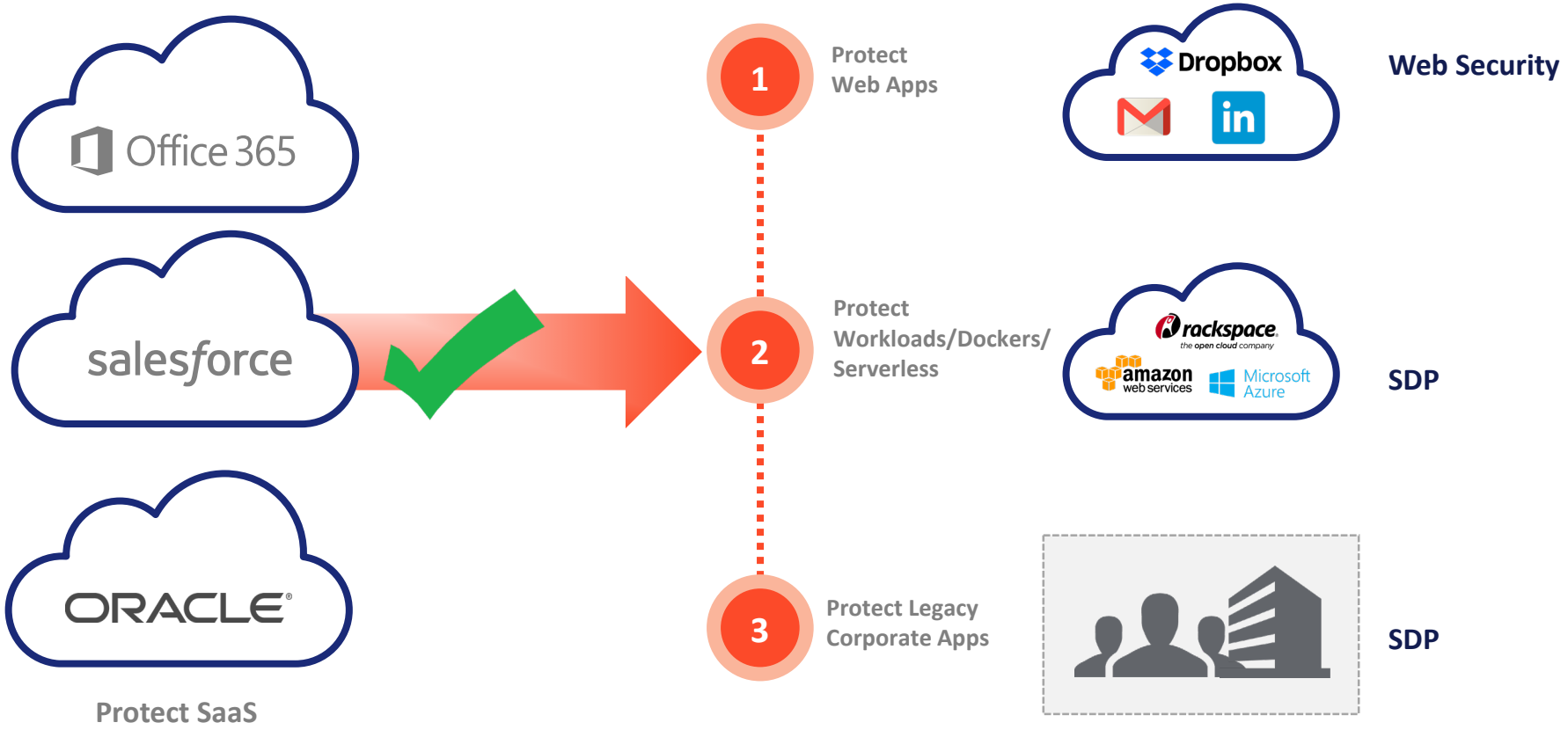
Rich SaaS visibility (logs, APIs & Gateway)

CASB as a comprehensive security platform

Challenge #1: Too Many Security Gateways



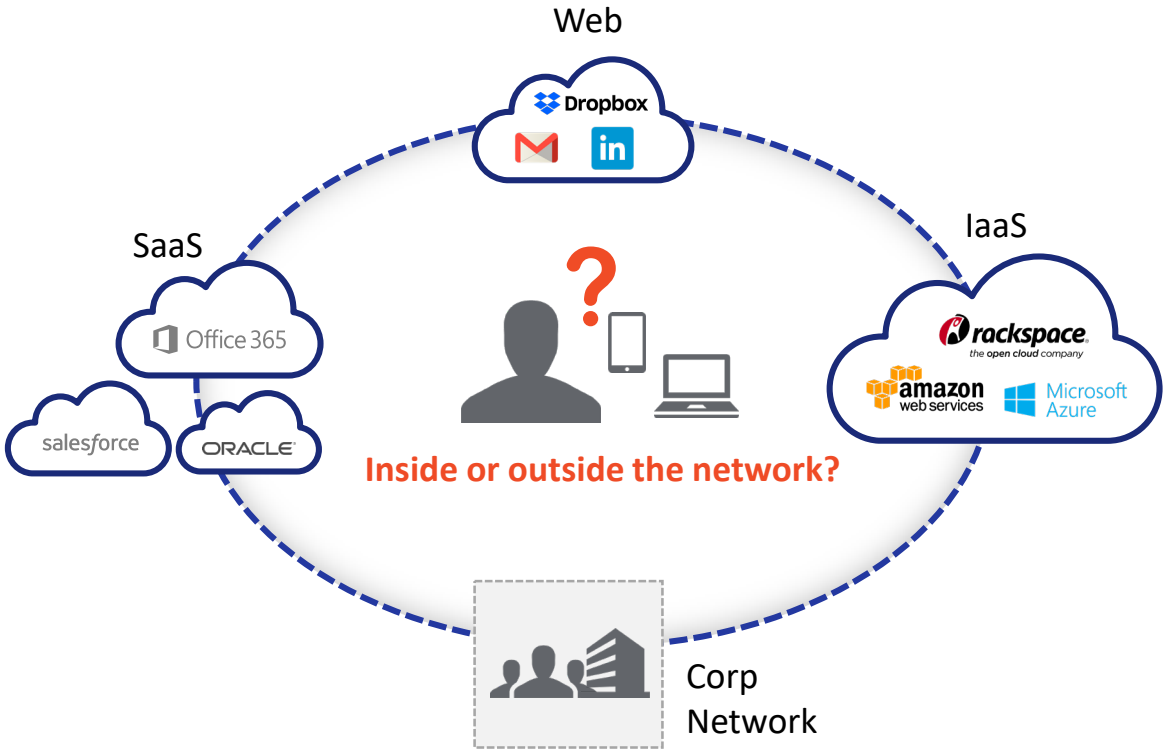
CASB to Evolve: Gateways Convergence



Zero Trust Principles Will Drive Convergence

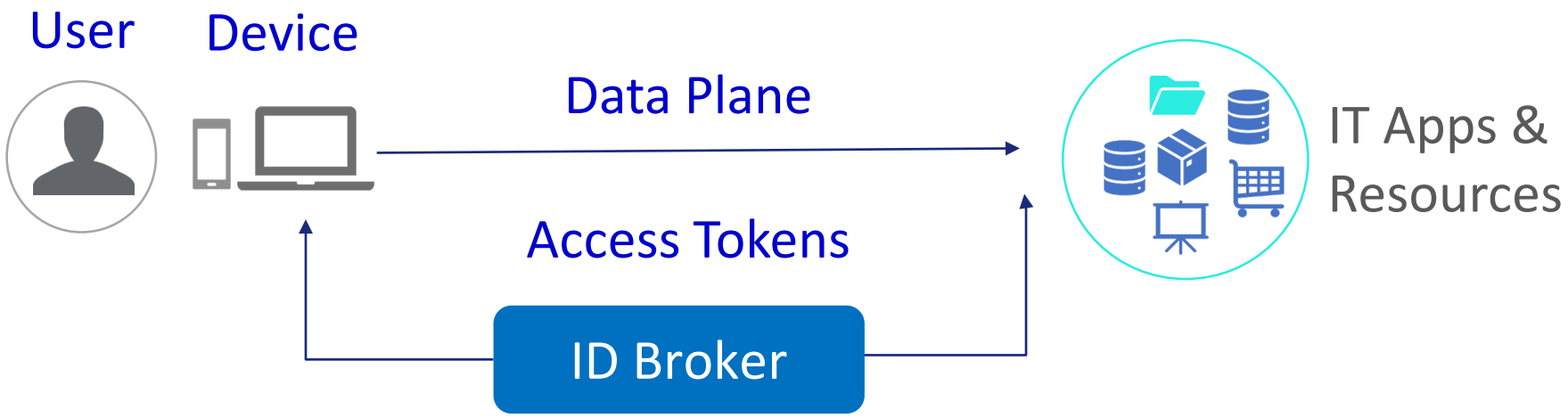
So What is Zero Trust & Software Defined Perimeter

In a world of cloud and mobile, what is the next network security blueprint?



The firewall is dead long live Zero Trust

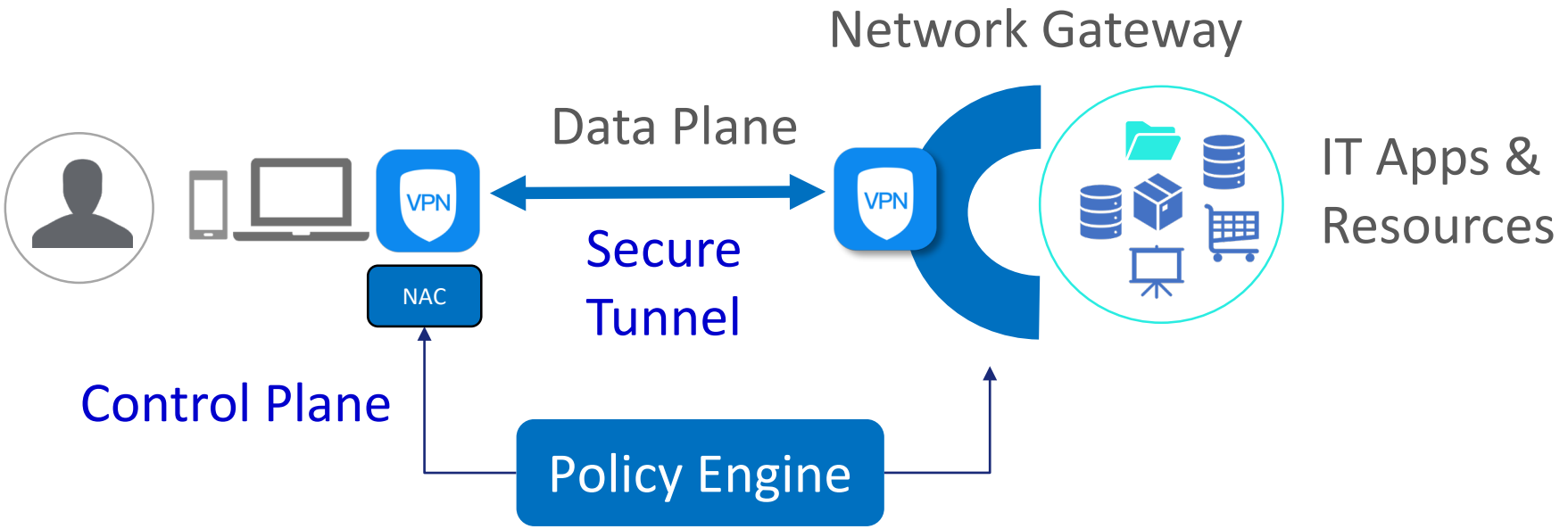
Zero Trust: Where the Identity Puck is Going



- **User:** Authenticate the user
- **Device:** Authenticate & verify (NAC) the device
- **Authorization:** Least privilege access

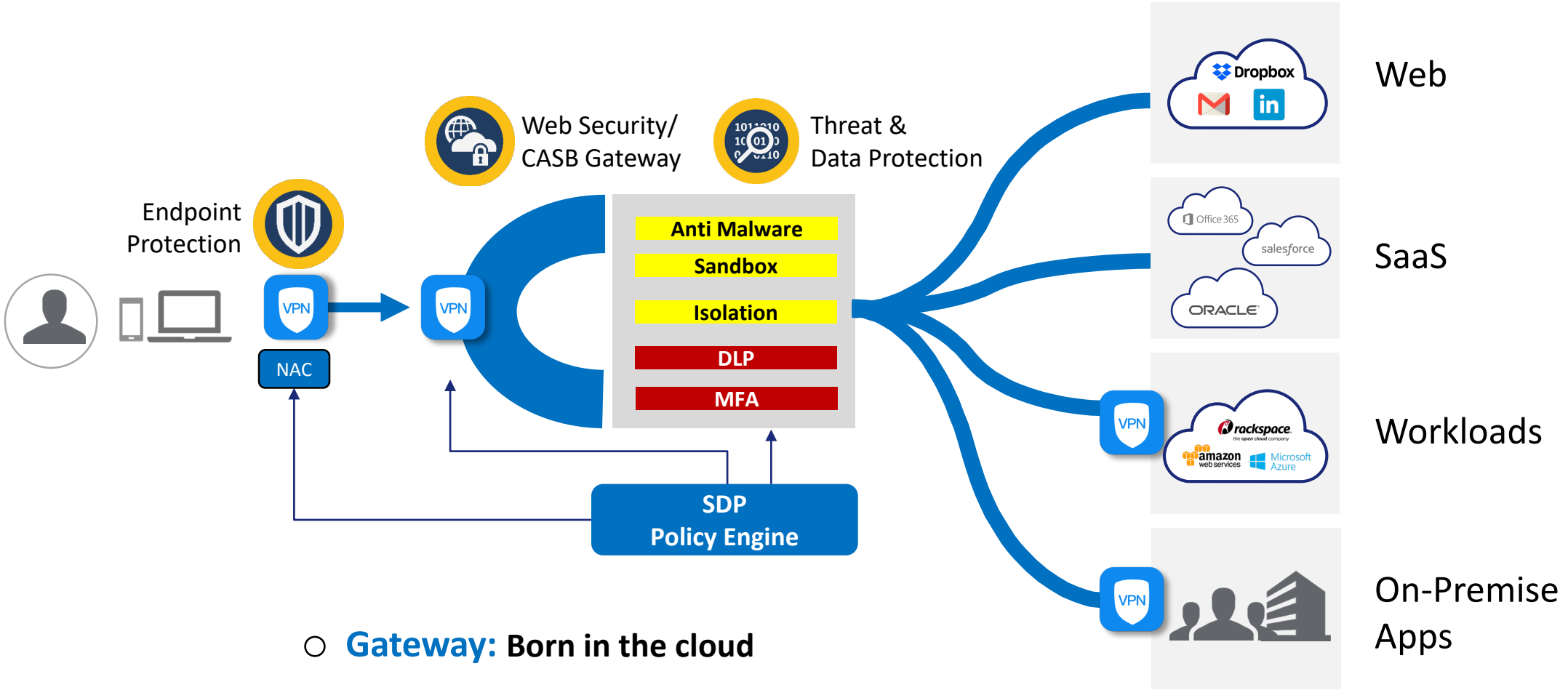
Zero Trust: Where the Networking Puck is Going

Software Defined Perimeter



- **Security Gateway:** Obfuscation& protection
- **Software-defined:** Separate control plane
- **Secure tunnels:** Point to point (opaque in Google BC)

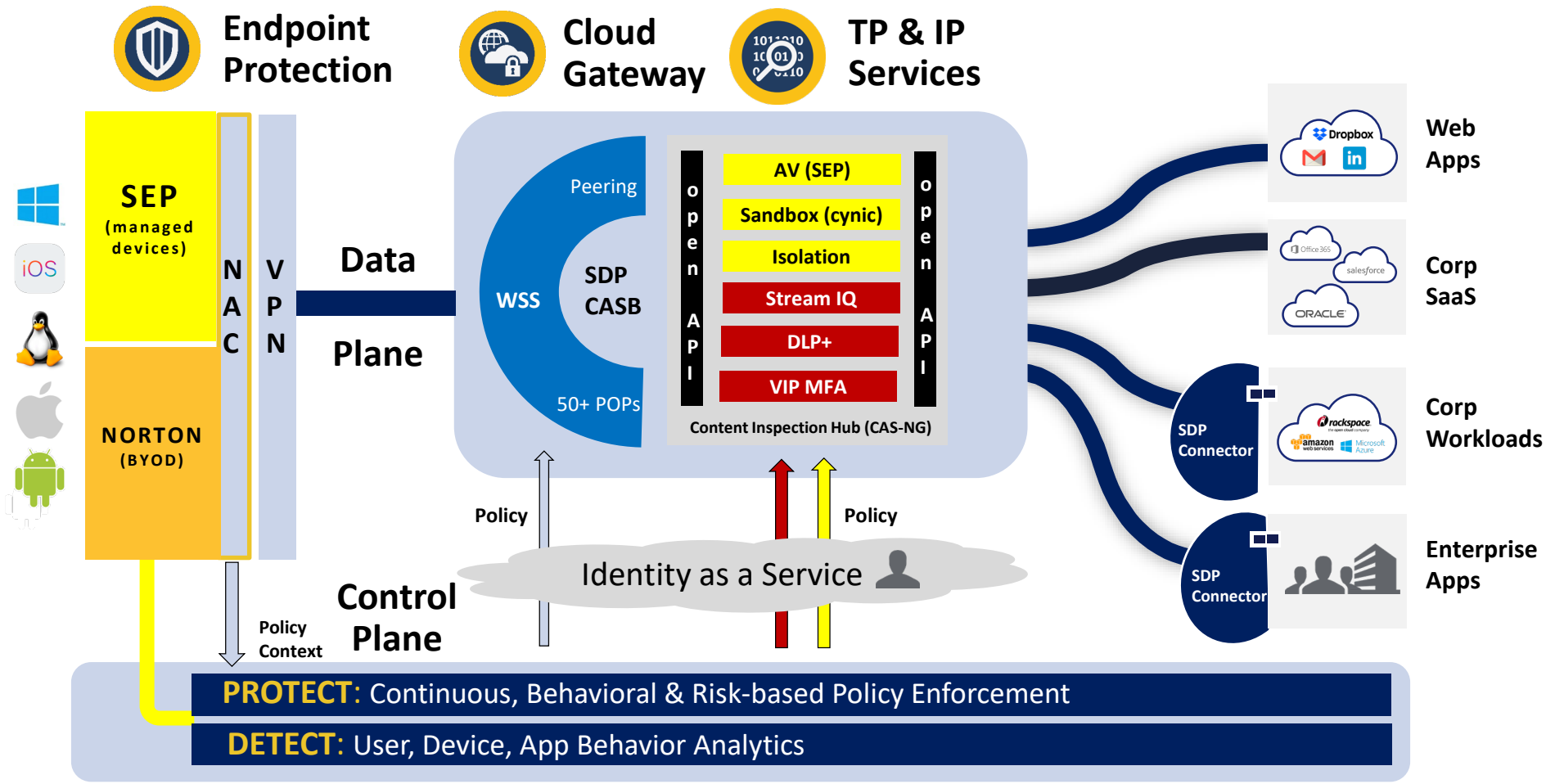
Symantec Point of View: “Beyond Corp”



- **Gateway:** Born in the cloud
- **Tunnel:** Not just secure, clean (content inspection)
- **Risk-assessment:** Continuous & adaptive (CARTA)

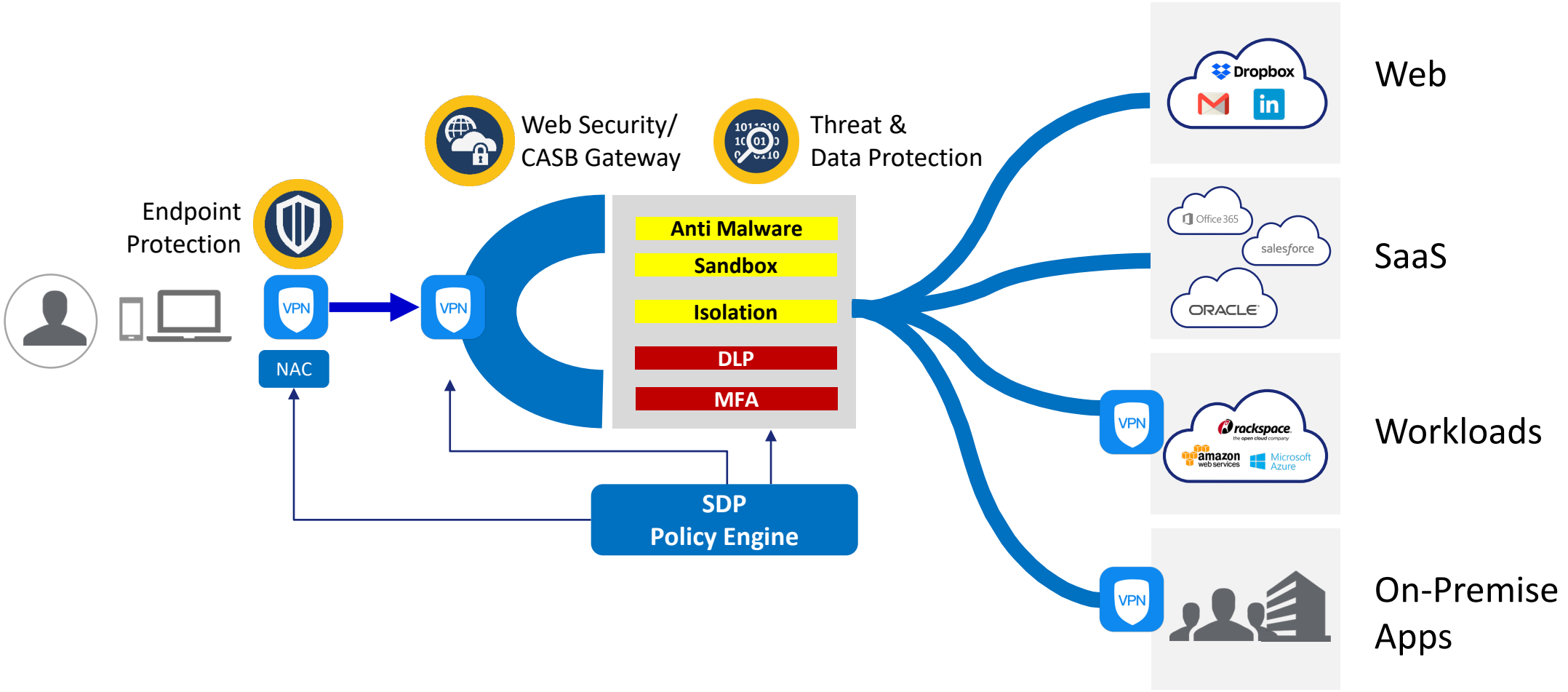
Symantec

From ”What” to “How”

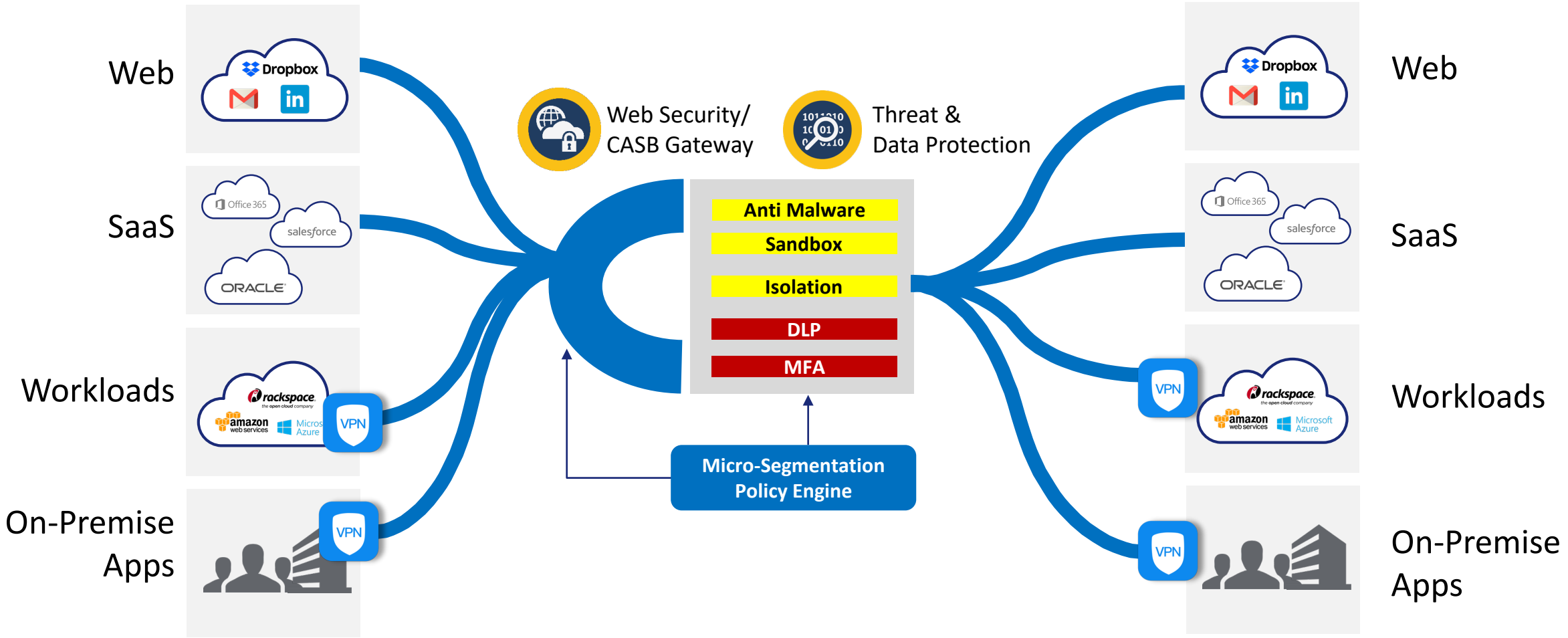


- **Endpoint Protection (AV, EDR):** Evolves as ZT agent with NAC and VPN capabilities
- **Web Gateways:** Unifies Web gateway with SaaS (CASB Gatelet) and Corp Apps (SDP) gateways
- **CASB:** Drives zero trust policy definition across unified gateway (WSS-Gatelet-SDP)

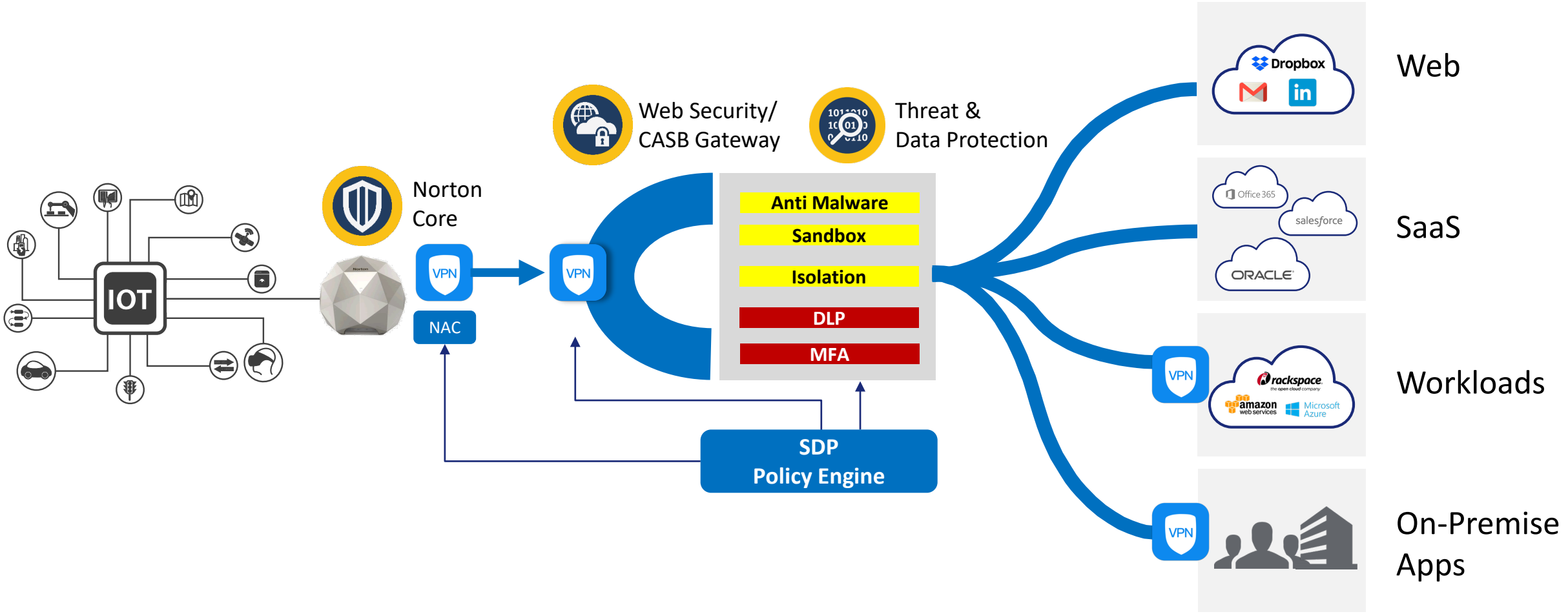
Powerful Use Cases: DevOps PAM (North-South)



Powerful Use Cases: Micro-Segmentation (East-West)



Powerful Use Cases: IOT Security (North-South)



Whoever Wins, One Gateway Problem Remains:

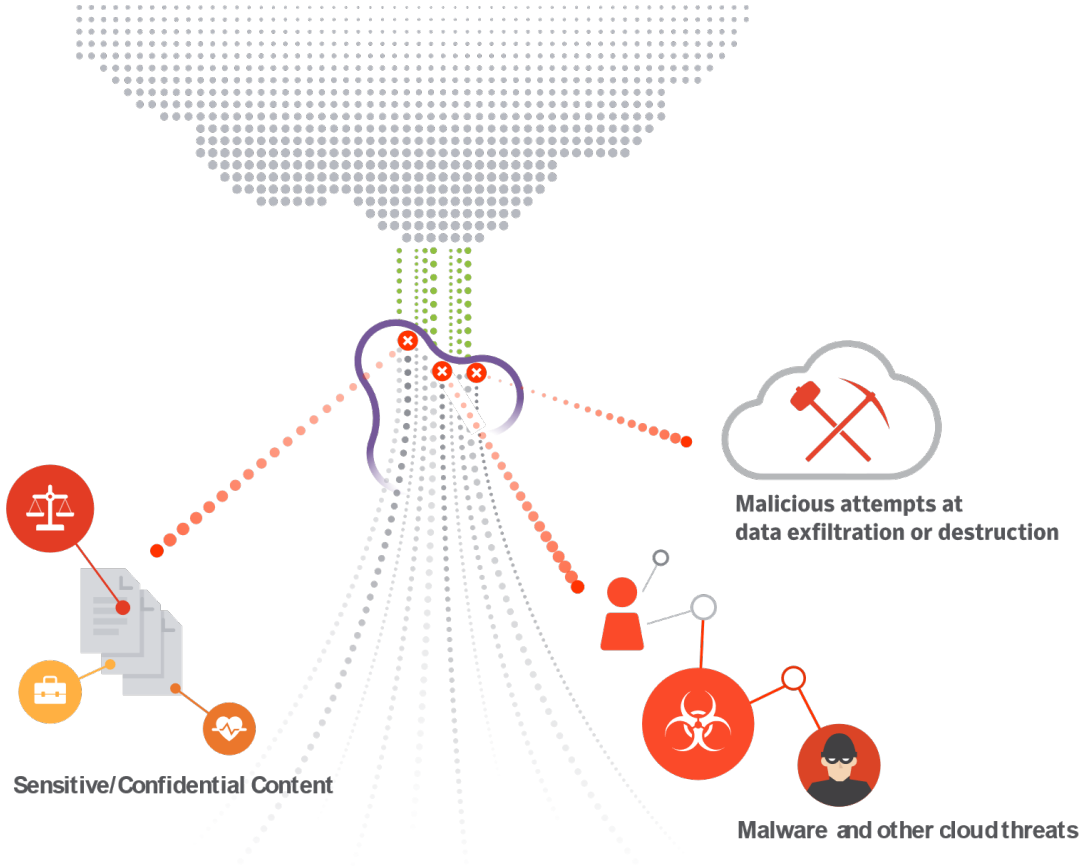
Unmanaged Devices & External Users

Today's Gateway Approach

	Sanctioned Apps	Unsanctioned Apps
Managed Devices	Forward Proxy	Forward Proxy
Unmanaged Devices	Reverse Proxy	N/A

Addresses a valid use case, but . . .

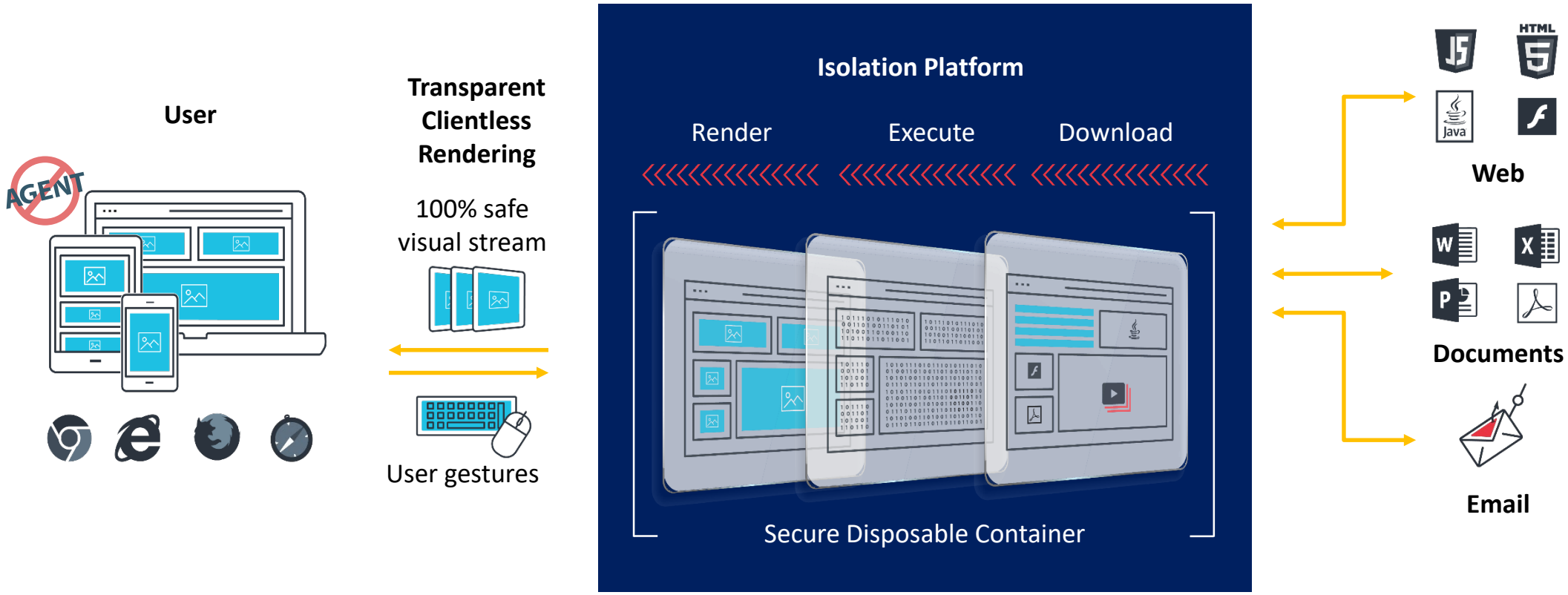
- Requires extensive URL rewriting
- Limited number of apps supported



The Third Approach: Mirroring

- No agent = any device
- No URL rewrite = any app

Crash Course: Web Isolation Technology



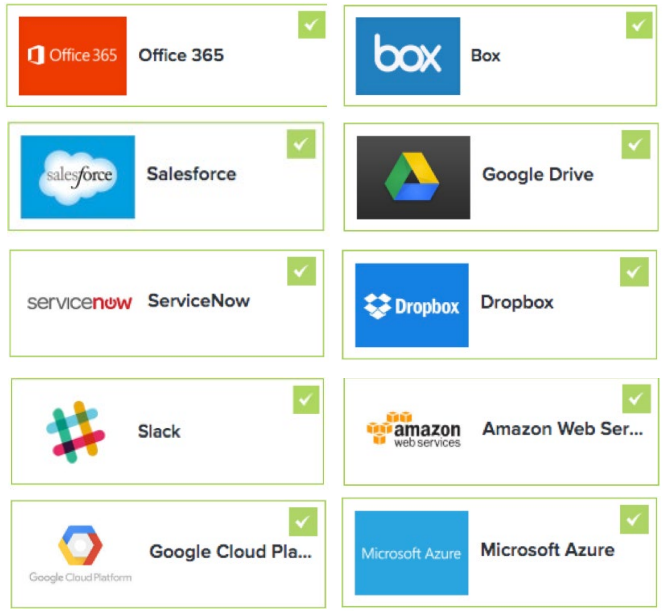
- Execute and render web sessions remotely
- Isolate both web and email, including attachments

DEMO -

https://clicktime.symantec.com/3ShmeUujHaikjjNRQeX6x5X7Vc?u=https%3A%2

Inline Coverage for Unmanaged Devices

Traditional Reverse Proxy



Mirror Gateway

+ Unlimited Apps Via Custom Gatelet

Conclusion: The Perimeter is Dead Long Live Cloud Defined Perimeter

- **CASB and SDP to Converge**
  - Security access brokering for ALL cloud apps
  - Obfuscation (private cloud)
  - NAC (all clouds)
  - Content inspection: everywhere!
- **Mirror Proxy to Complement RP and FP**

  Inline, real-time access security brokering
  - ALL sanctioned cloud apps
  - ALL unmanaged devices