

RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PART3-T11

Unshackle Legacy Security Restrictions for 2020 and Beyond

Tom Gillis

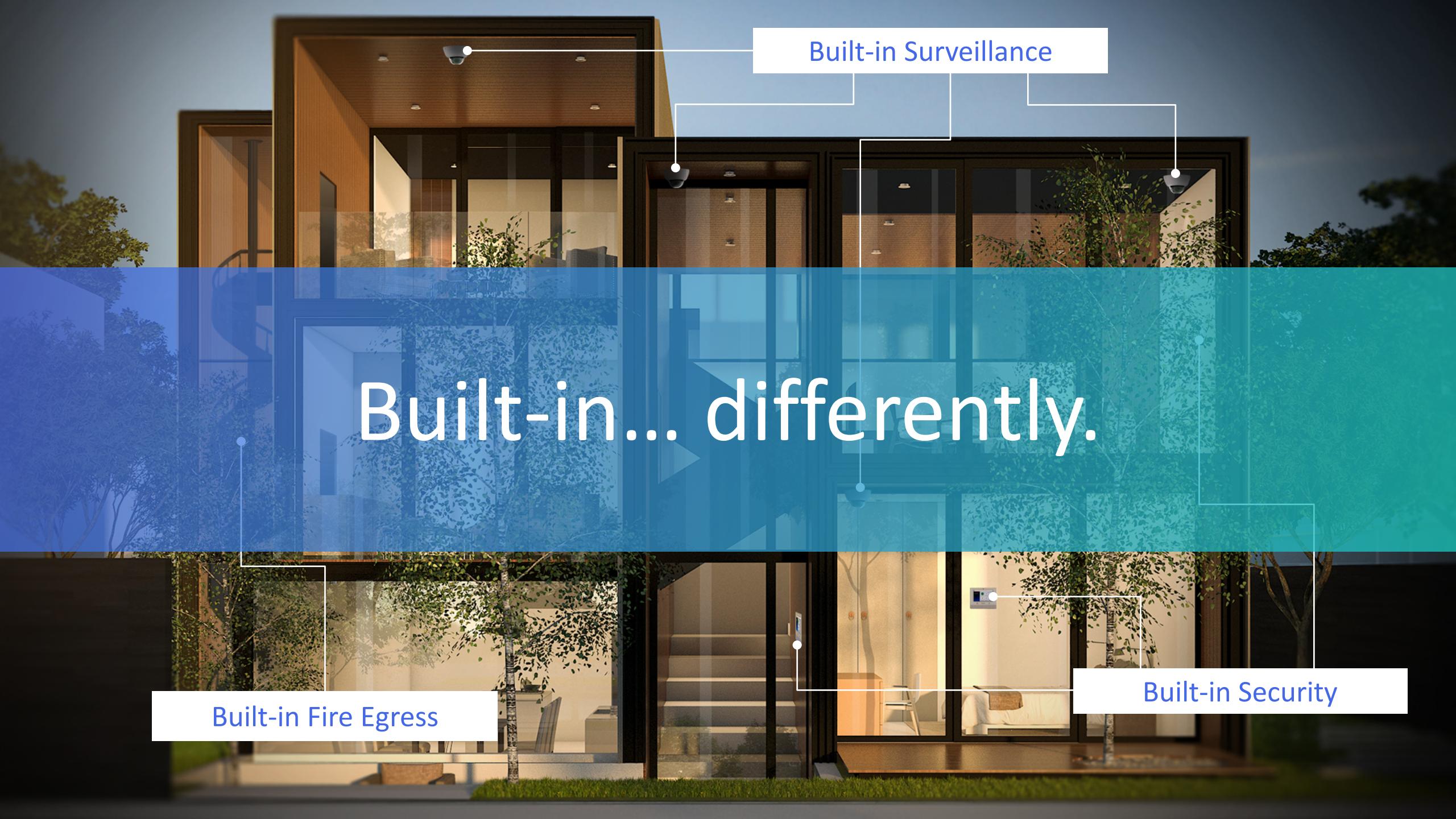
Senior Vice President / General Manager
Networking and Security Business Unit
VMware



#RSAC



Bolted on.



Built-in Surveillance

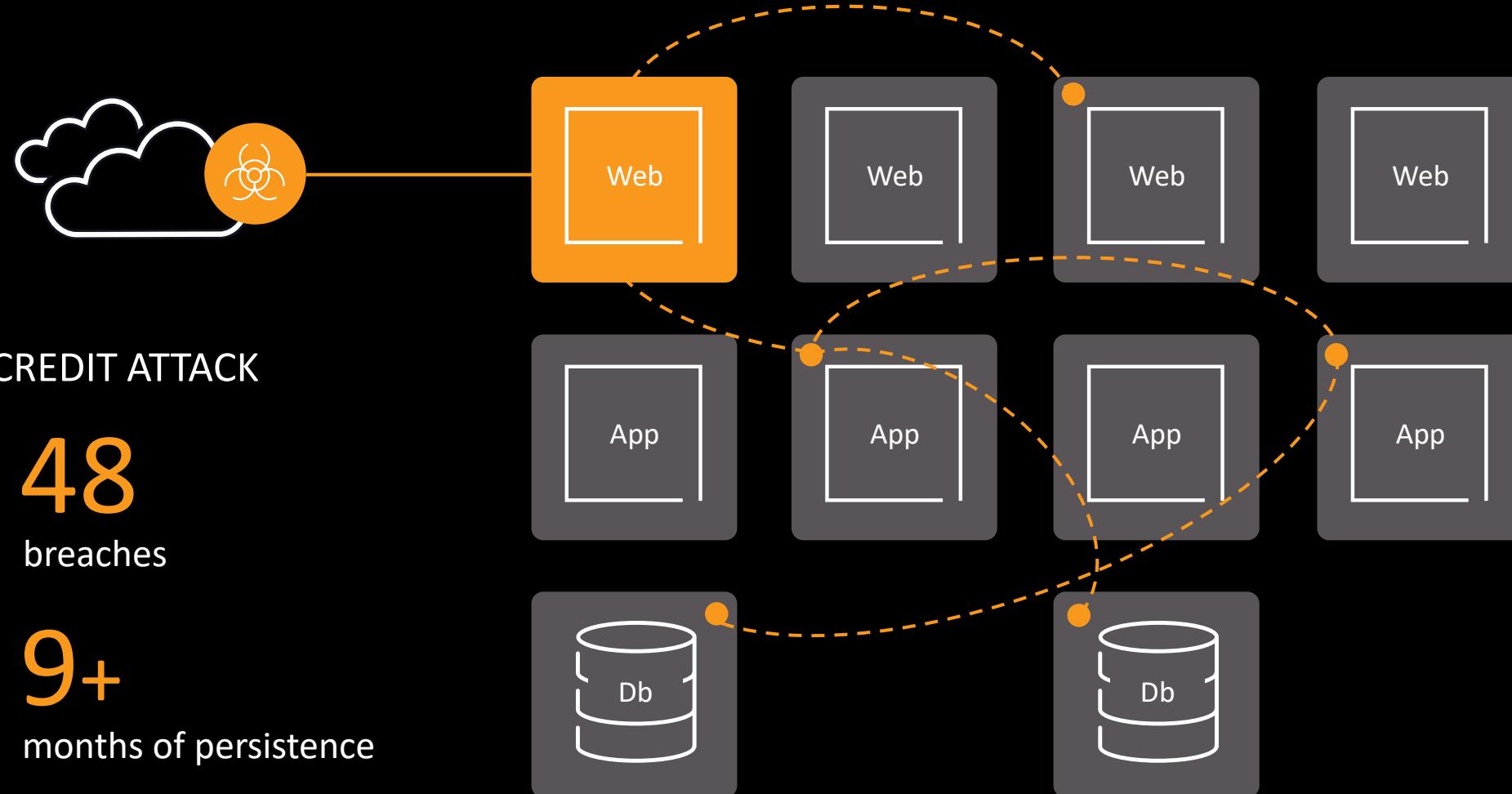
Built-in... differently.

Built-in Fire Egress

Built-in Security

The Power of Intrinsic

East-West is the new battleground



Major Financial Institution Attack

\$3.5B

Market value erased after data breach
was announced

Key Report Insights

Attacker Behavior

Defense Evasion

90%

of attacks in 2019 used defense evasion behaviors

Ransomware's Resurgence

60+%

of ransomware attacks are targeting critical infrastructure

Defender Behavior

IT / Security Dynamics

50%

of IT and security teams said they are currently understaffed

77%

said IT & security have a negative relationship

Maintenance and Integration

55%

said driving collaboration across IT and security teams should be the organization's top priority over the next 12 months

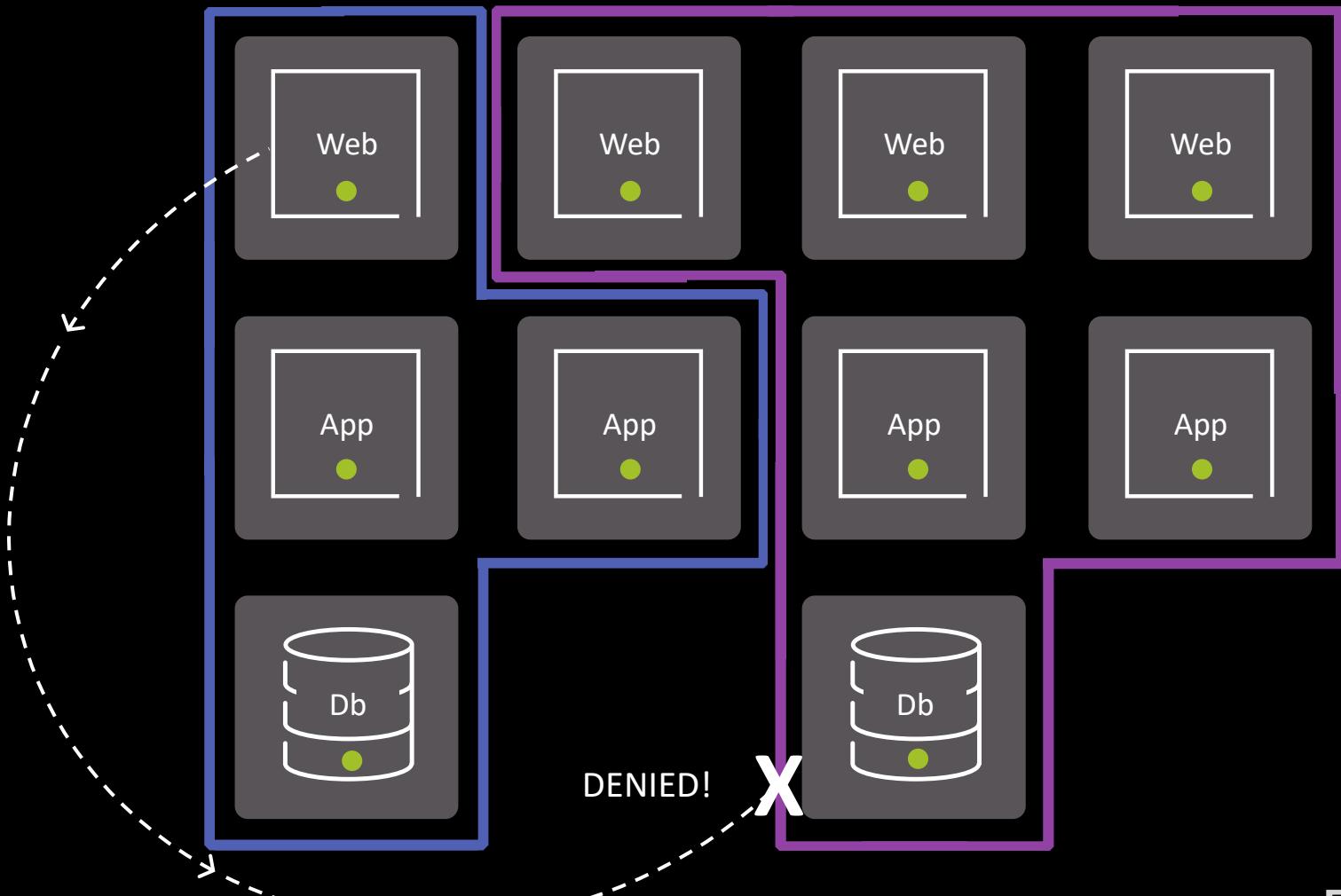


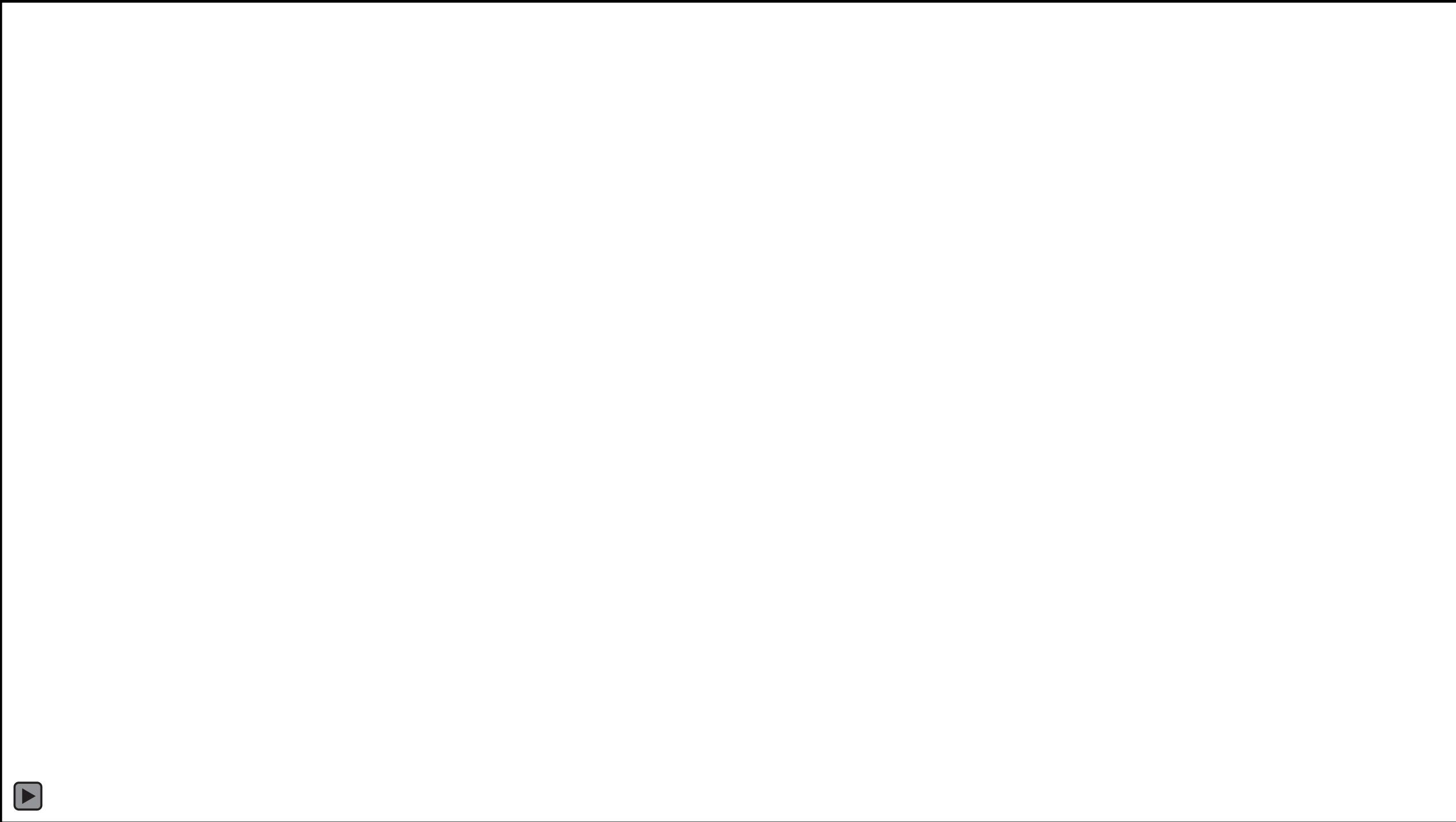


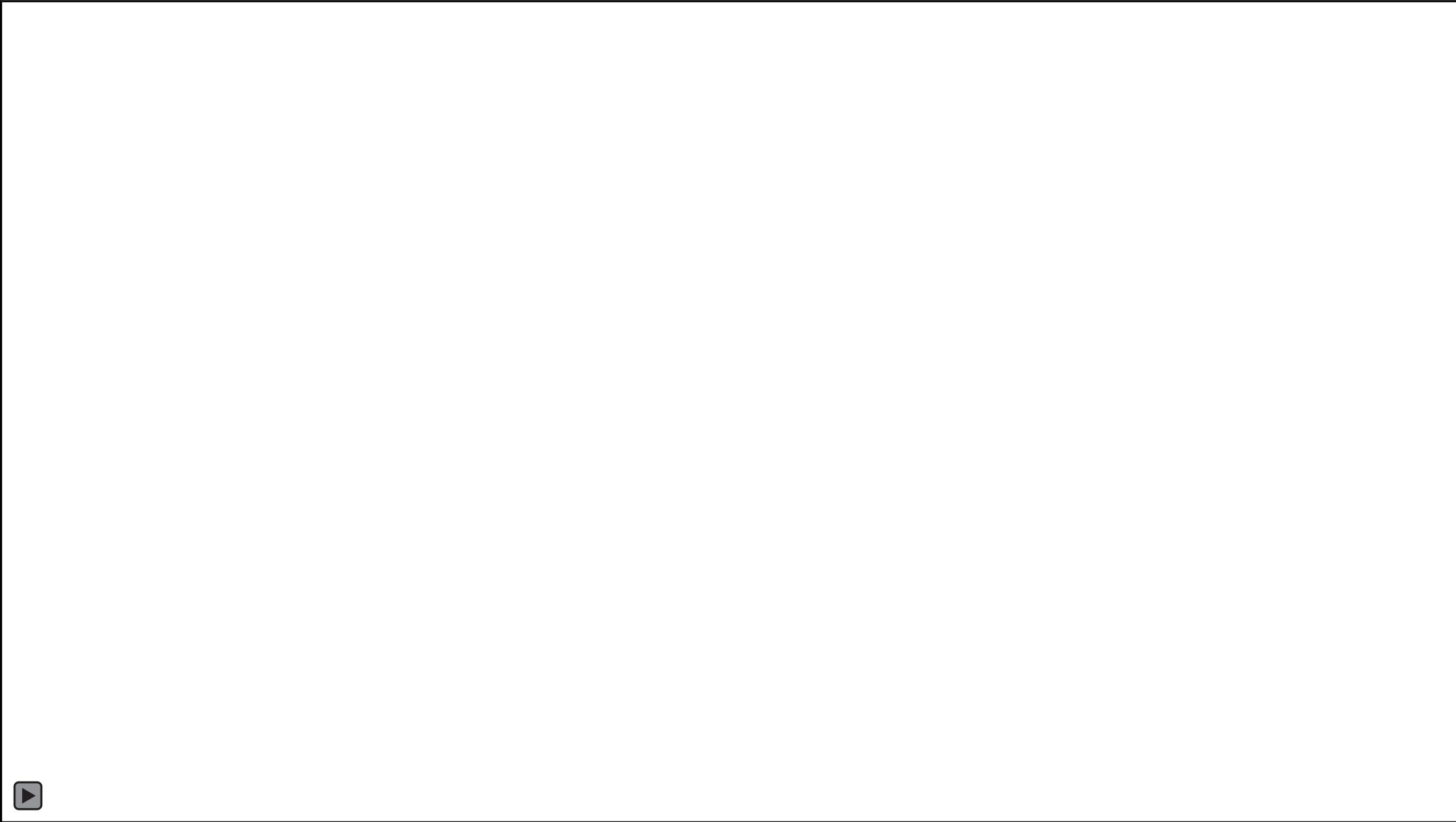
NSX Intelligence

The Power of Intrinsic

Making E/W micro-segmentation work

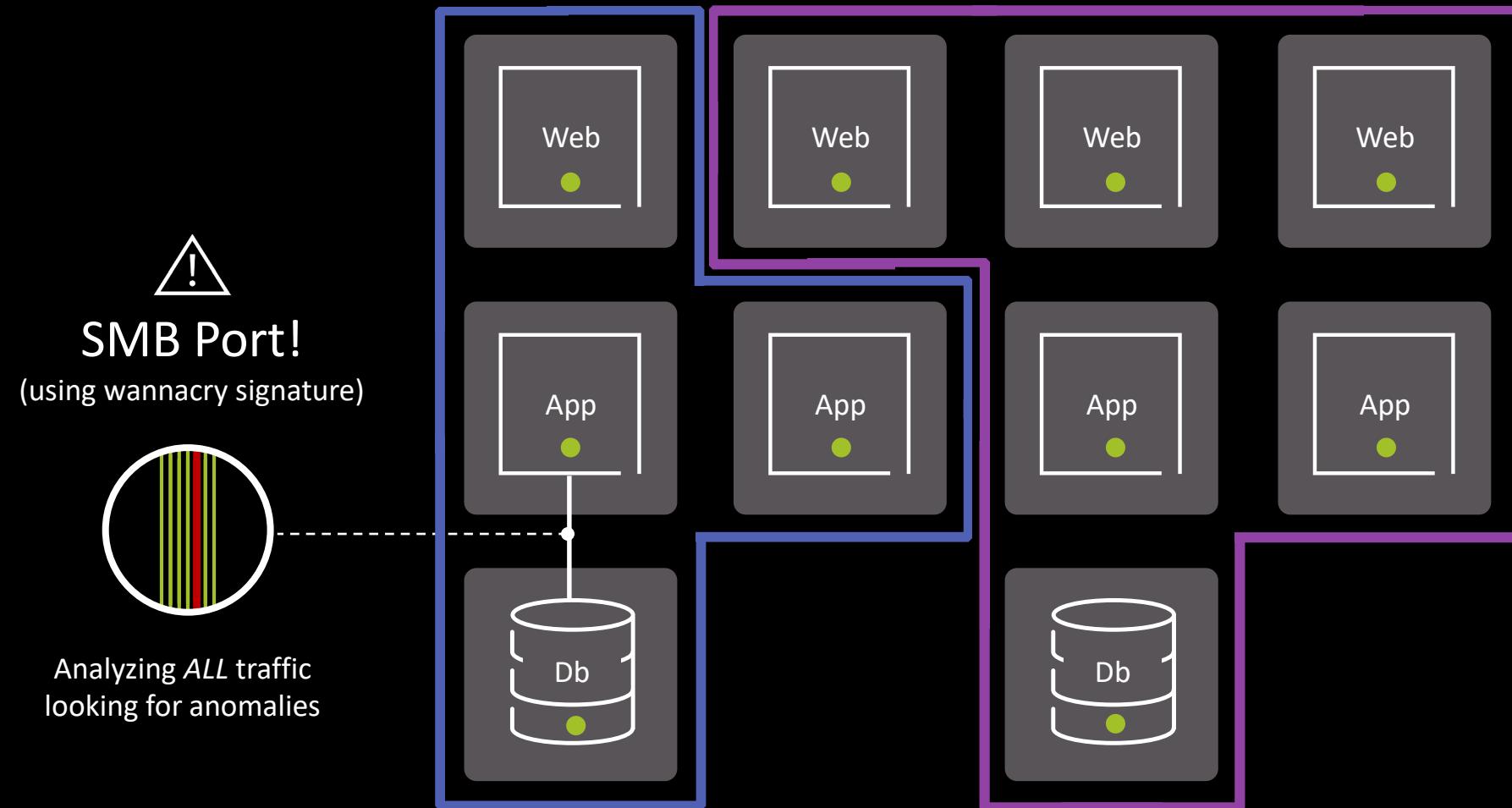






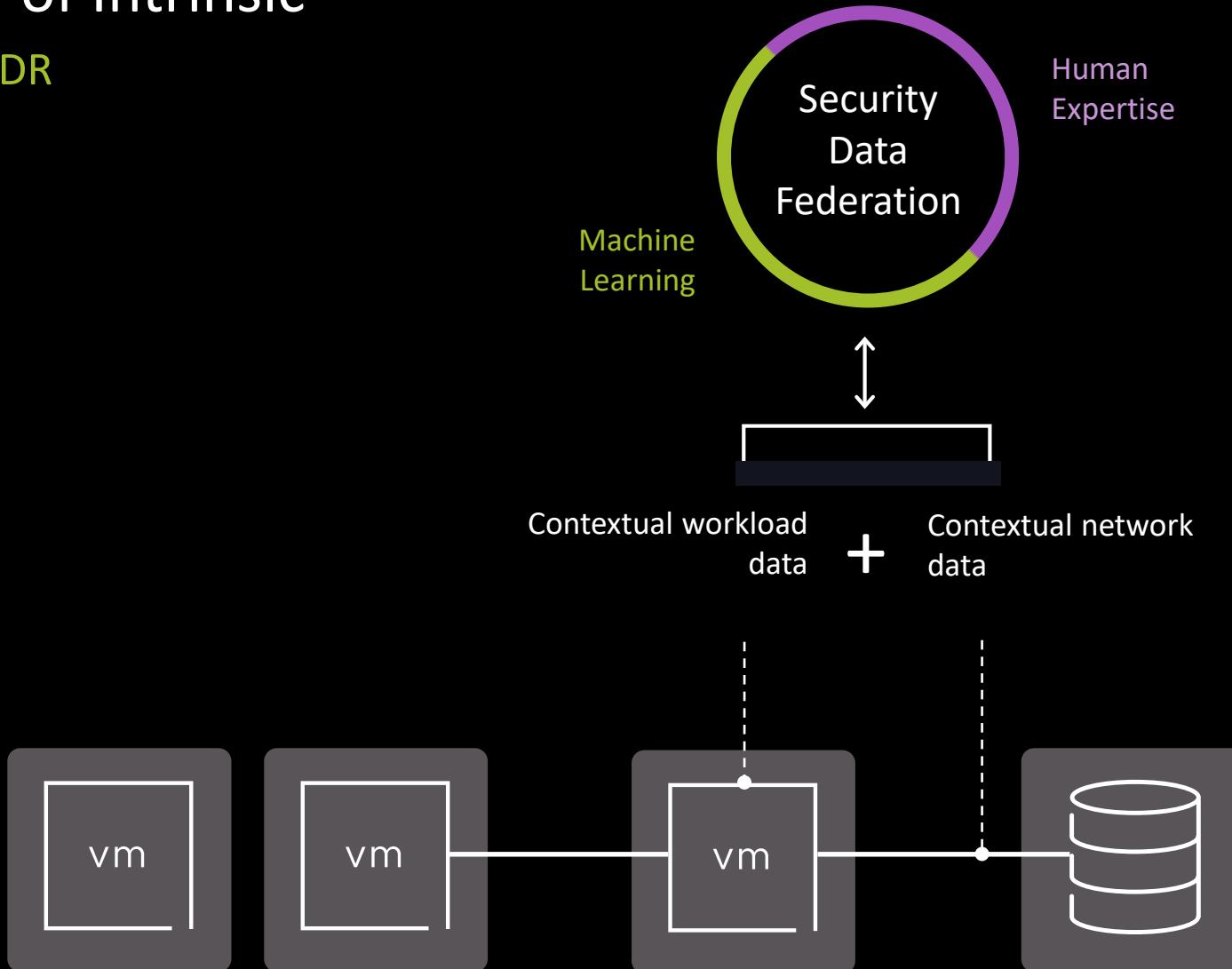
The Power of Intrinsic

From port blocking to E/W inspection



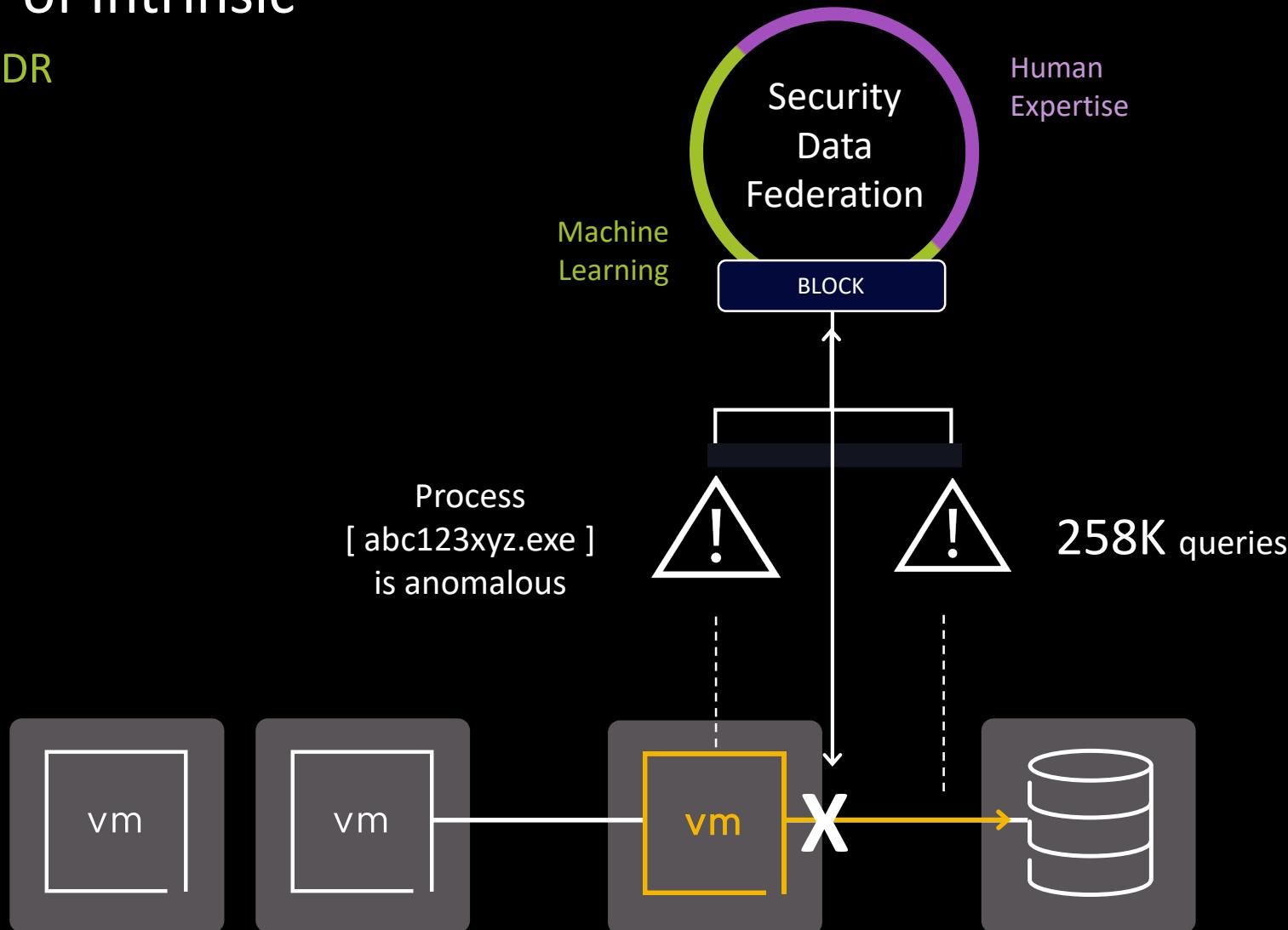
The Power of Intrinsic

EDR + NDR = XDR

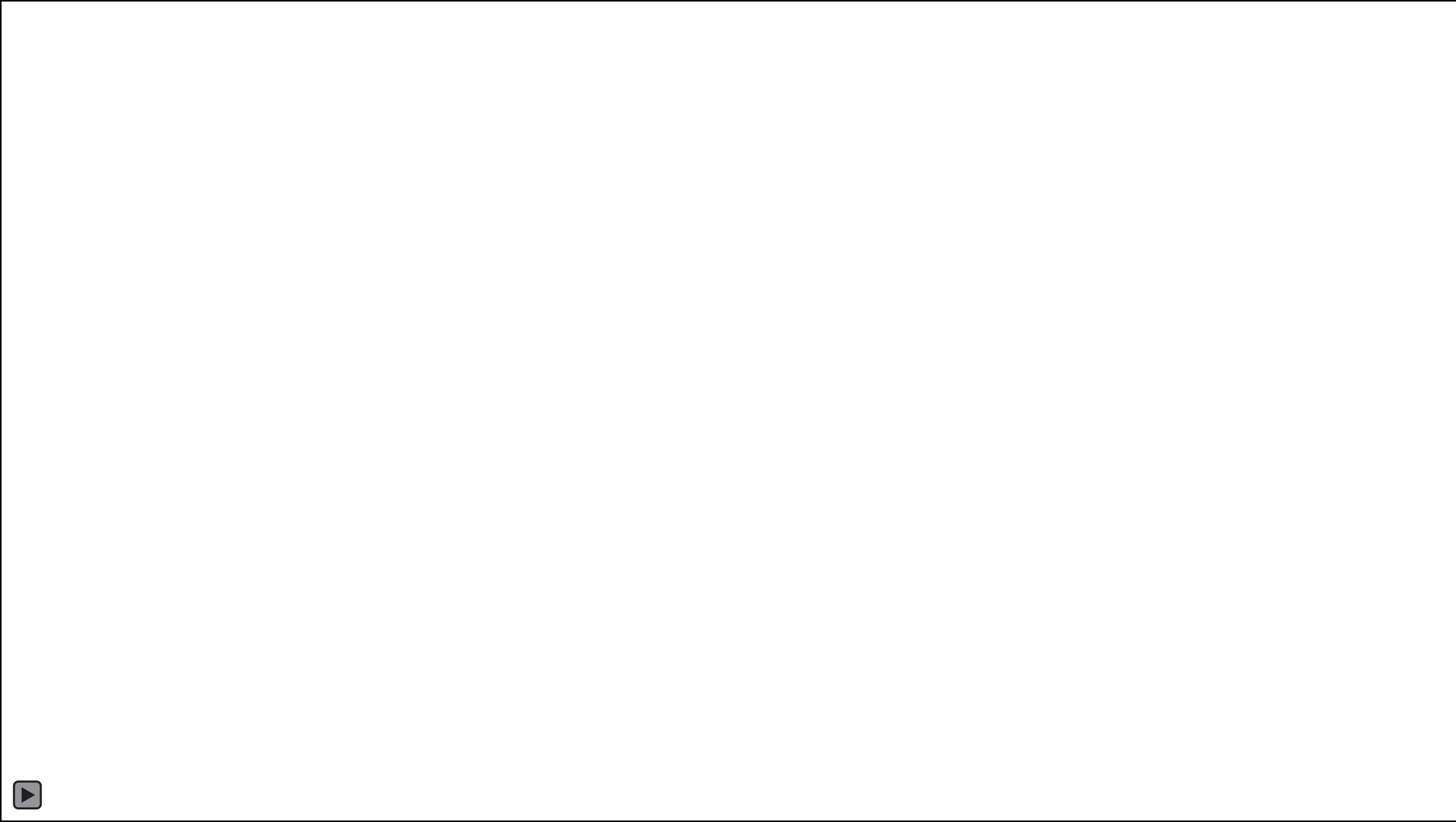


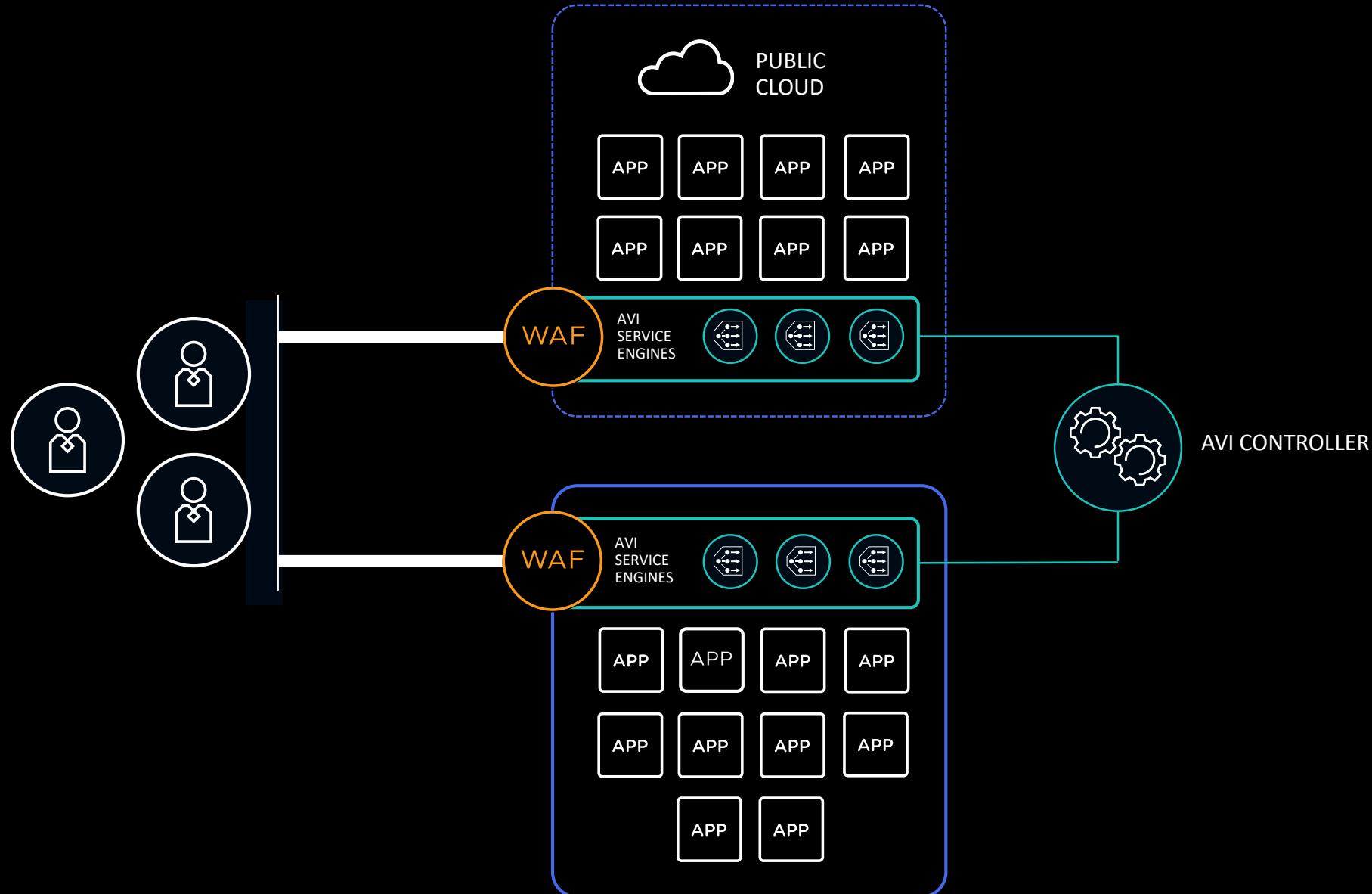
The Power of Intrinsic

EDR + NDR = XDR







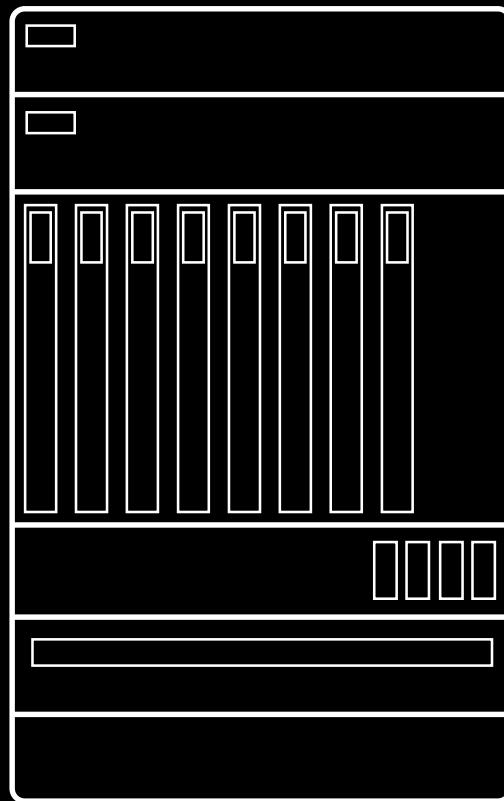


Paris DC

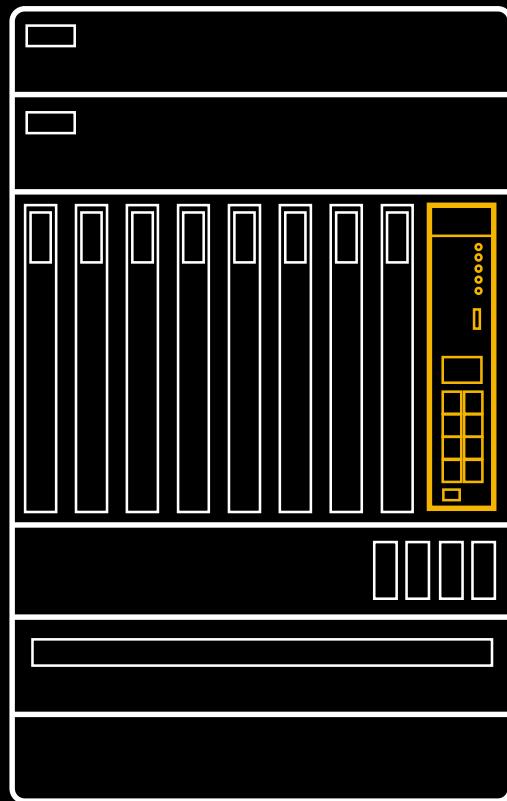
RSA® Conference 2020

The end of the
Black Box Era!

INTEGRATED = BOLTED ON



INTEGRATED = BOLTED ON



Same firewall...
...repackaged.







IDS/IPS SIGNATURES

<SIGNATURE><SIGNATURE><SIGNATURE>

Finance_app IDPS

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

Apache IDPS

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

<SIGNATURE><SIGNATURE><SIGNATURE>

MySQL IDPS

<SIGNATURE><SIGNATURE><SIGNATURE>

Finance_app

Web_tier



42

Tomcat

35

Exchange

132

Apache

• From 13k signatures...
>80%* signatures evaluated at each IDPS engine

Finance_db



AD Server

56

NOTE: Figures are approximate, for illustrative purposes only.

Finance_app

Web_tier



Firewall Rules



WAF Rules

Finance_db



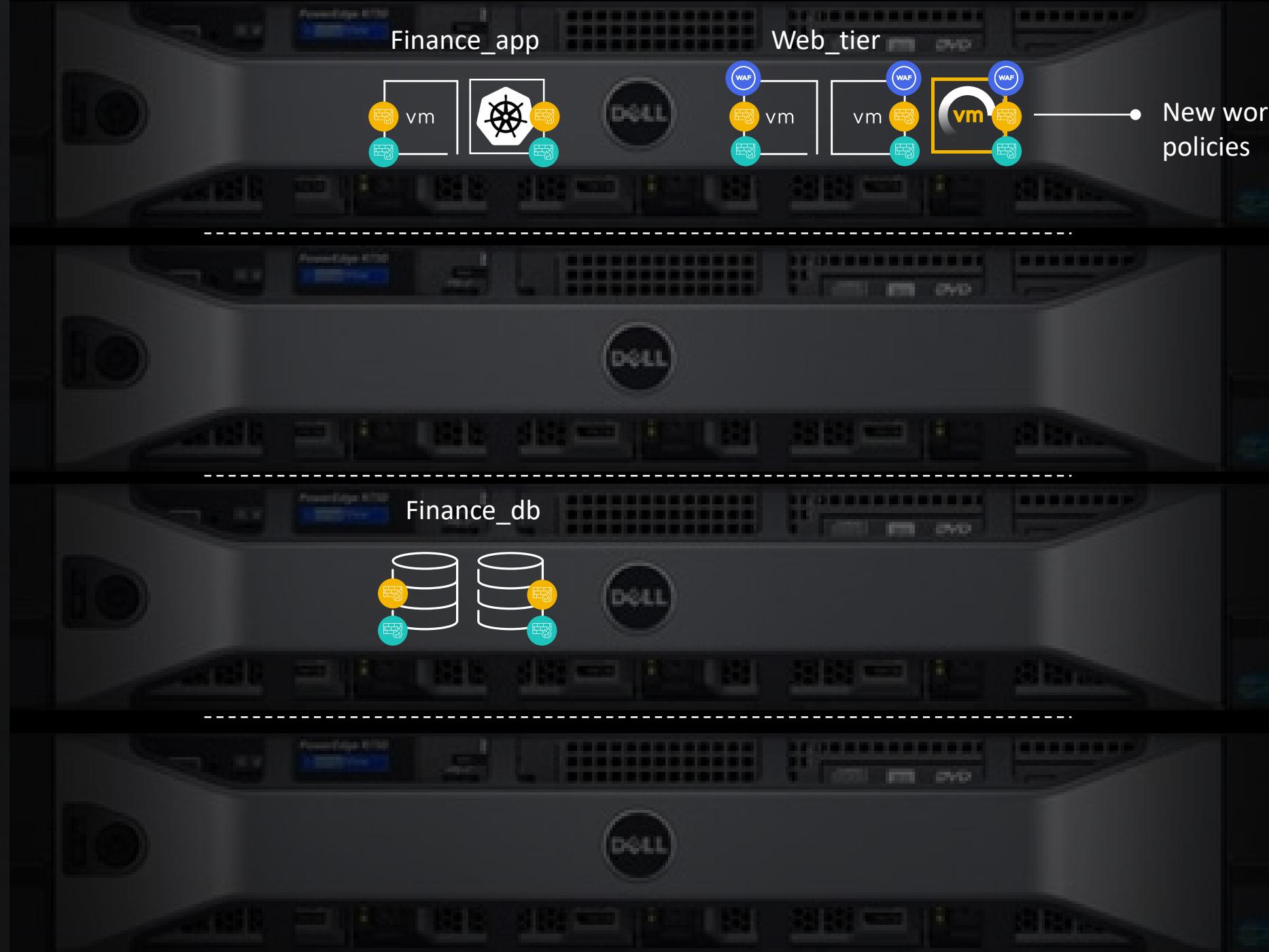
Finance_app

Web_tier



Finance_db

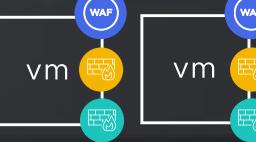




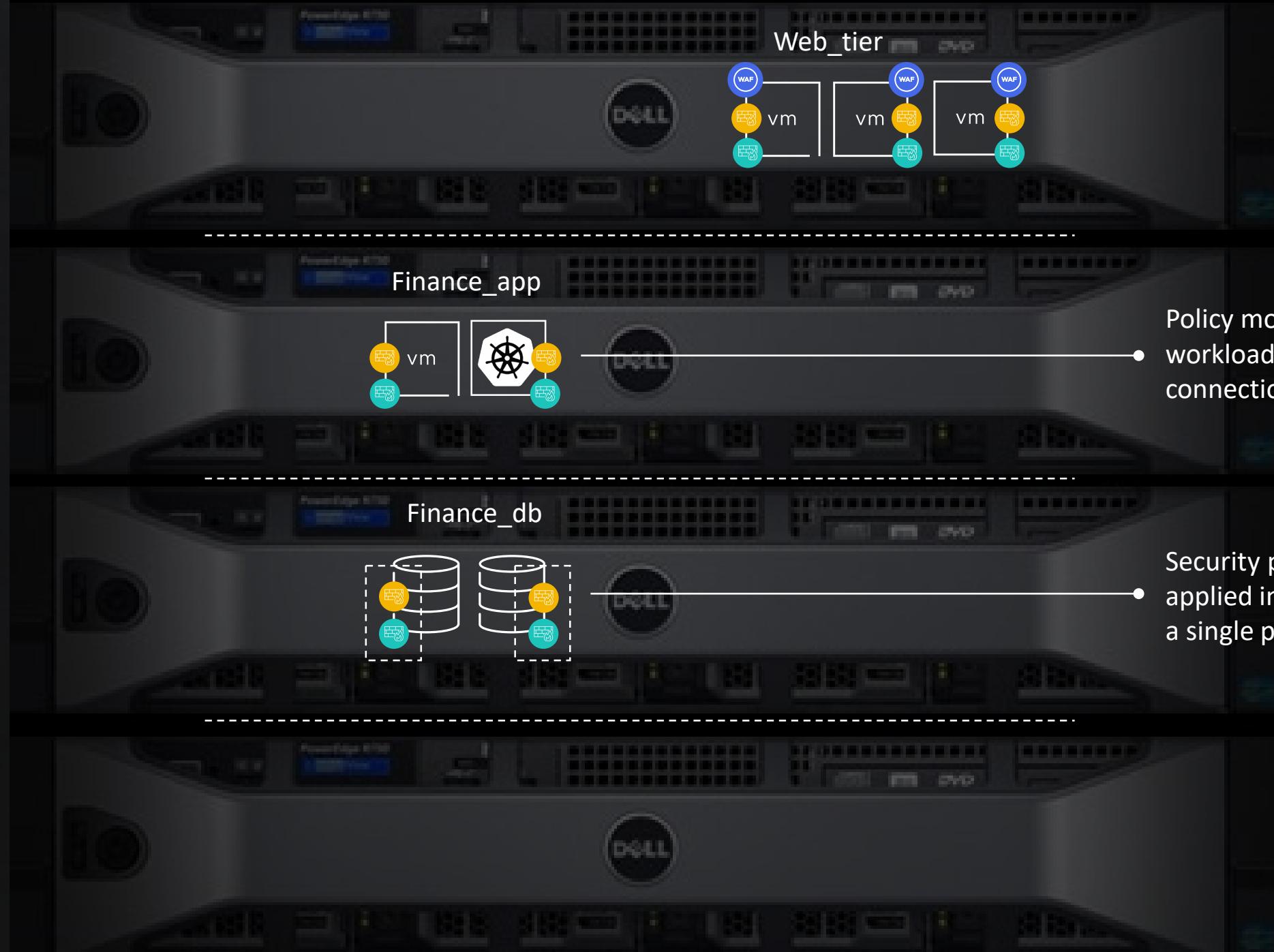
- New workloads inherit policies

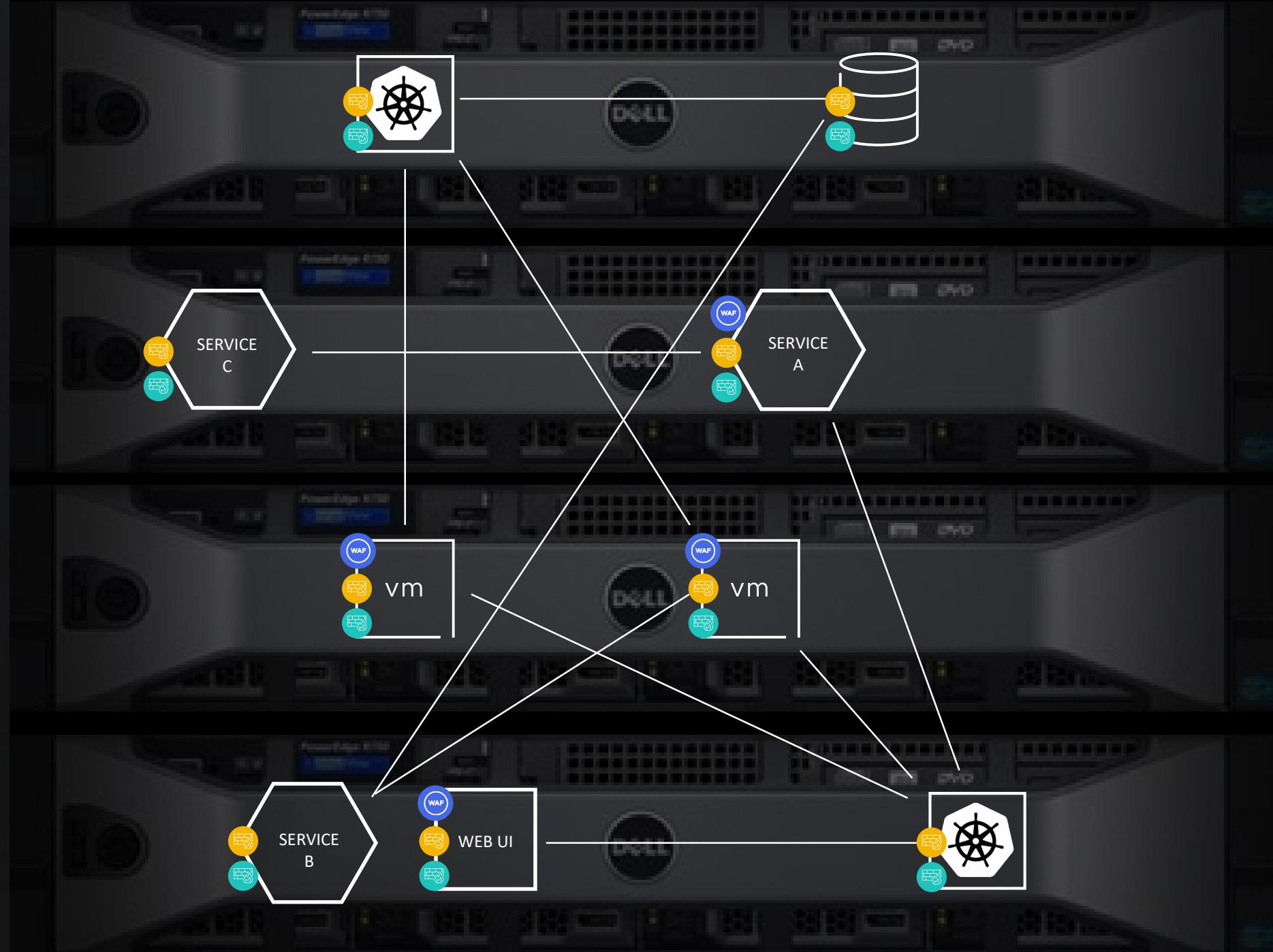
Finance_app

Web_tier



Finance_db





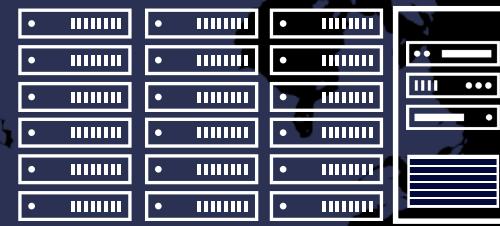
vm



= First Class Citizens

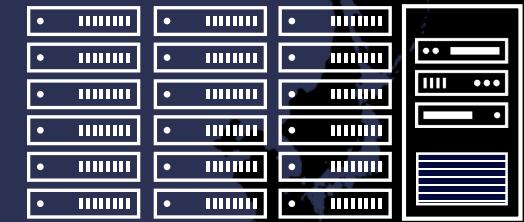
Federated

NEW

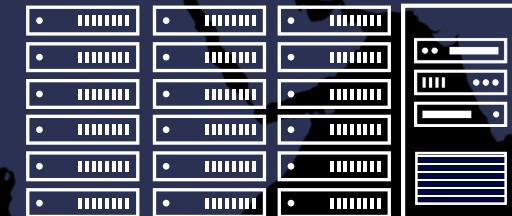


DC 1

Global Manager



DC 2



DC 3

Allow globally
dispersed deployments

Zone
stretching

Workloads can move
locations

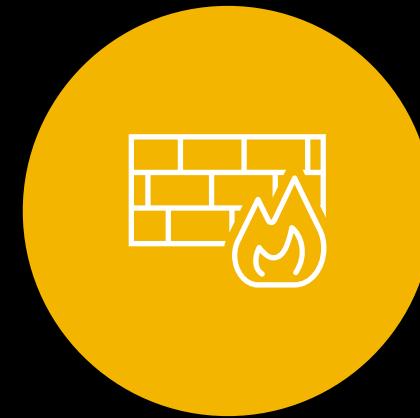
VMware Advanced Security for Cloud Foundation



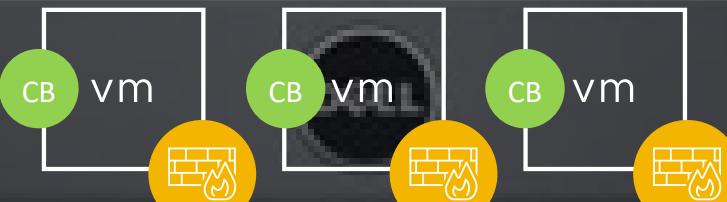
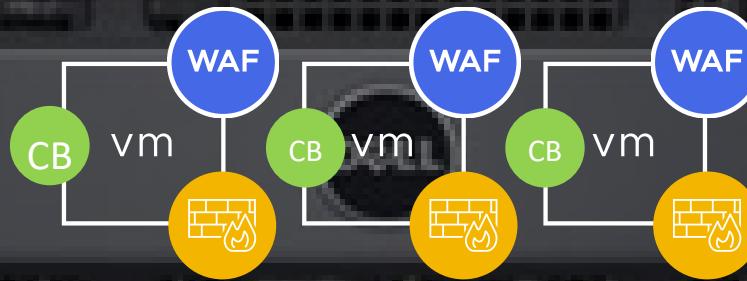
VMware Carbon Black
Technology



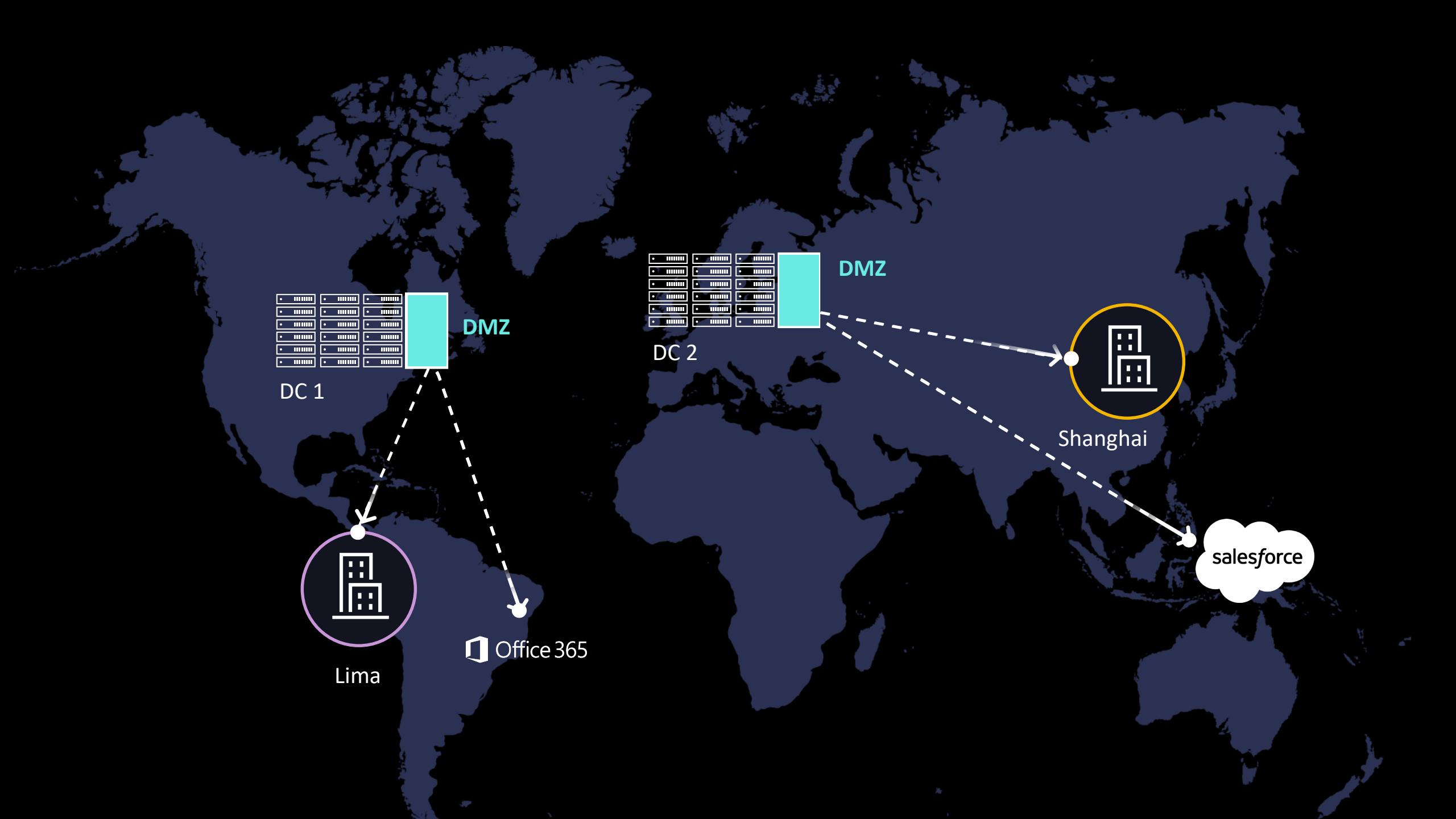
VMware NSX Advanced Load
Balancer/WAF

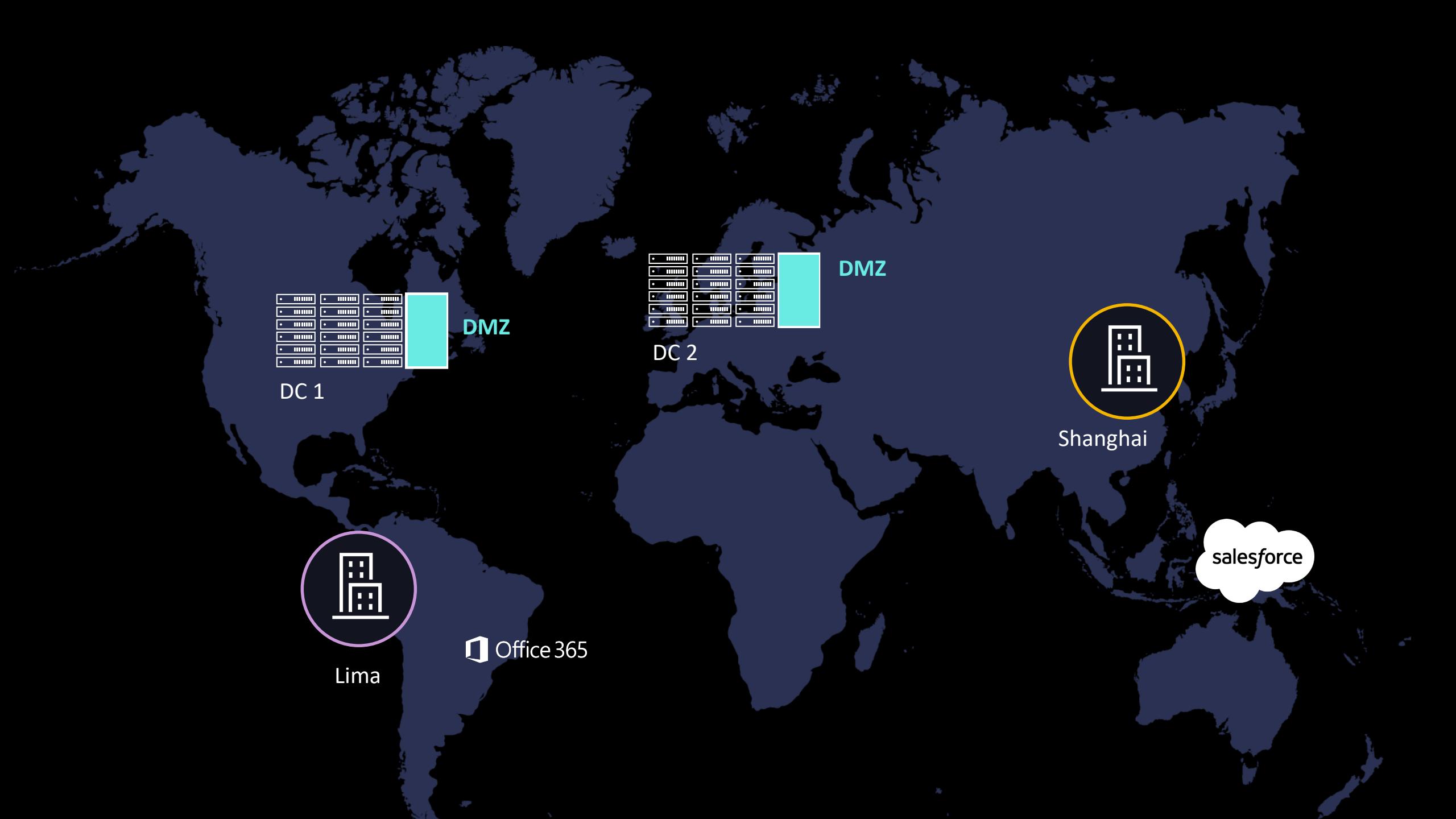


VMware NSX Distributed
IDS/IPS

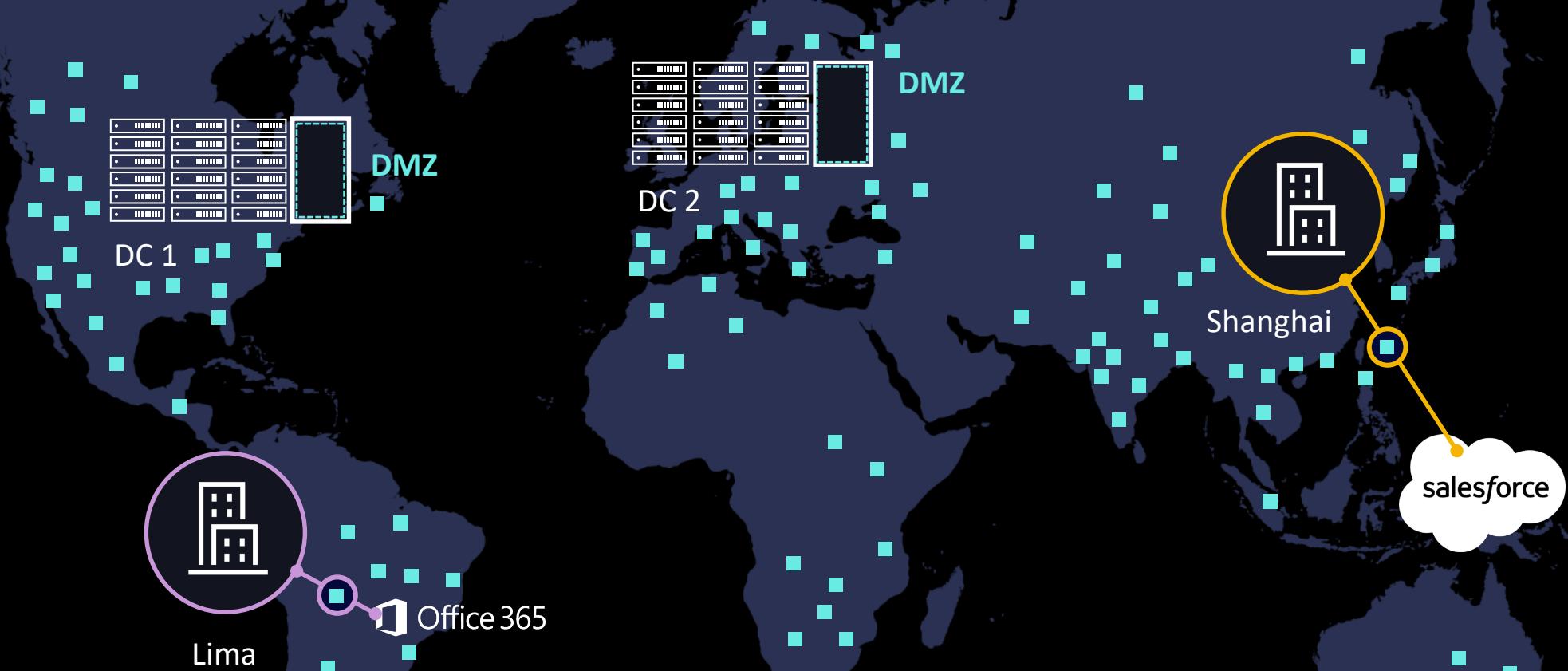


- VMware Carbon Black Technology
- Service-defined Firewall IDS/IPS
- Advanced Load Balancer / WAF





Secure Access Service Edge (SASE)



Demo

Get Your Copy of the Cybersecurity Threat Report And Learn More About Enhancing Your Security at:

VMware (booth #6145)
Carbon Black (booth #5873)

The collage includes several screenshots from the report:

- A top-level page featuring a man in glasses looking at a screen, with network traffic analysis on the right.
- A section titled "Top Malware Behaviors of 2019" with a bar chart showing:

Behavior	Percentage
Software Packing	26%
Hidden Windows for Command & Control (C2)	22%
Standard Application Layer Protocol	20%
Registry Keys in the Startup	15%
Process Discovery	17%
- A "Behavior Spotlights" section with a "Software Packing" entry:

 - Definition: Software packing is the act of compressing an executable file or program into a smaller file or executable file.
 - Description: Attackers often use software packing to hide their malicious intent. It's a common technique used by malware authors to obfuscate their code and make it more difficult for security researchers to analyze.
 - Advice to Defenders: Defenders should be aware of software packing techniques and use tools to detect and analyze packed files.

- A "Defender Evasion: Hidden Windows" entry:

 - Definition: Hidden windows are windows that are not visible to the user. They are often used by attackers to perform tasks without being noticed.
 - Description: Hidden windows can be used by attackers to perform tasks such as keylogging, stealing sensitive information, or launching attacks. They are often used in conjunction with other evasion techniques like process hollowing or thread hijacking.
 - Advice to Defenders: Defenders should be aware of hidden windows and use tools to detect and analyze them.

RSA® Conference 2020

Thank You