The Journey to Zero-Trust

Security Beyond The Perimeter

Ray Heffer

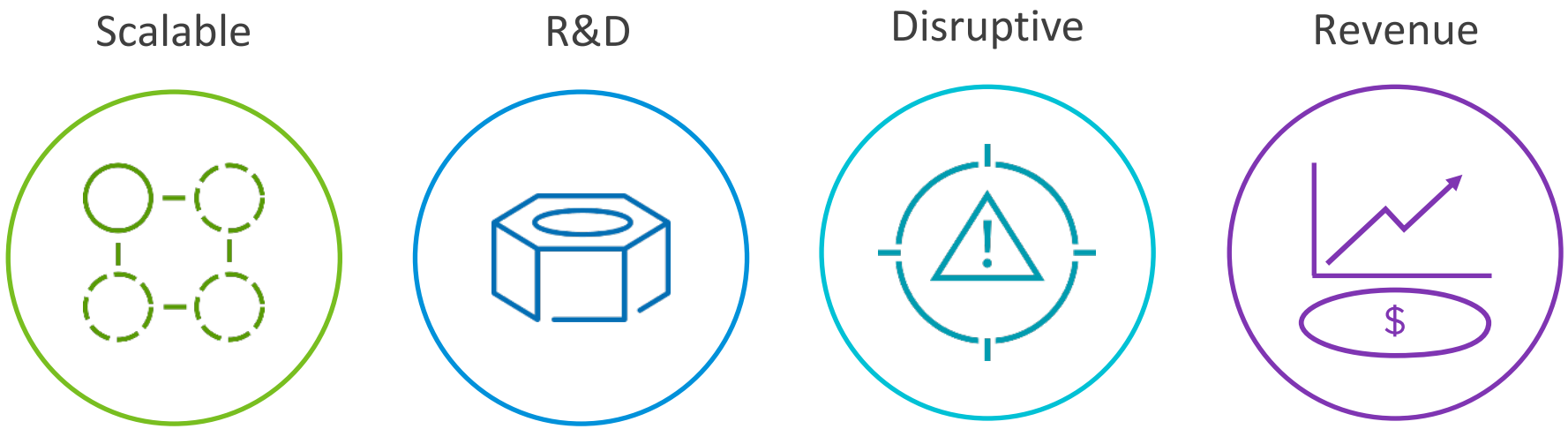
Field CISO, Cybersecurity Strategist

Certified Ethical Hacker, VCDX #122

Twitter: @CISOops

- What Does Zero-Trust Actually Mean?
- The Persistent Threat of Ransomware
- VMware's Zero-Trust Journey
- Key Takeaways
- Q&A

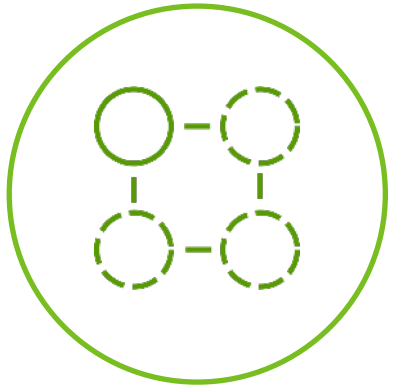
Ransomware-as-a-Service (SaaS) Security



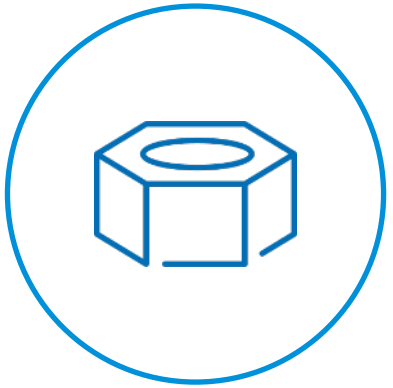
Reverse Engineering Ransomware Motives

Let’s work backwards

Scalable



R&D



Disruptive

Revenue


Zero Trust for the Enterprise

Zero-Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise owned network boundary.

Zero-Trust Principles:

- **Assume** there is **No Implicit Trust** granted to assets or accounts based solely on physical or network location
- **Authentication** and **Authorization** (both subject and device) are discrete functions performed before a session is even established.
- **Protect** resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Five Pillars of Zero-Trust

Device Trust	User Trust	Data Trust	Application Trust	Transport Trust
• Patch Management • Compliance State • AD Domain-less Operation • EDR and Antimalware • Endpoint Firewall	• Certificate-Based authentication • Multifactor Authentication • Conditional and Least Privilege Access	• Full Disk Encryption • Data Loss Prevention (DLP)	• SSO • Encrypted Connections • Micro-Segmentation • VDI • App-Specific Tunnels	• Micro-Segmentation • Transport Encryption • Session Protection

VMware Workspace ONE®
VMware Carbon Black®
VMware Horizon® View™
VMware NSX®

Visibility and Analytics (Security Information and Event Management [SIEM], Log Insight)

Security Orchestration and Automation (SOAR)

Every

2 seconds

a new organization falls victim [2]

59%

of all attacks involve double extortion

>4000

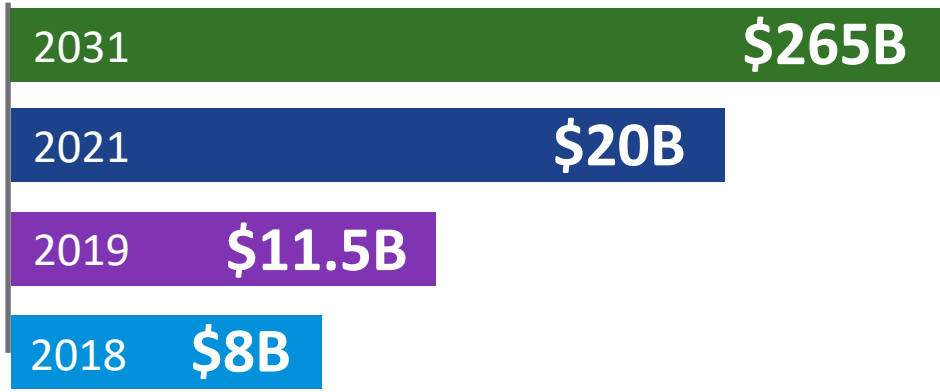
ransomware attacks happen daily [1]

Full funded adversary syndicates

Ransomware

As-a-service

Damage [3]



[1] Justice.gov

[2] Cybersecurity Ventures (Oct, 2019)

[3] Cybersecurity Ventures (Oct. 2019)

60%

of organizations surveyed were hit by ransomware in the last 12 months[1]

92%

Didn’t regain full access to their data following a ransom payment[2]

16 days

Average downtime following a ransomware attack[3]

55%

Will manage core, edge and cloud data protection from the cloud by 2025[4]

[1] VMware Global Incident Response Threat Report 2022

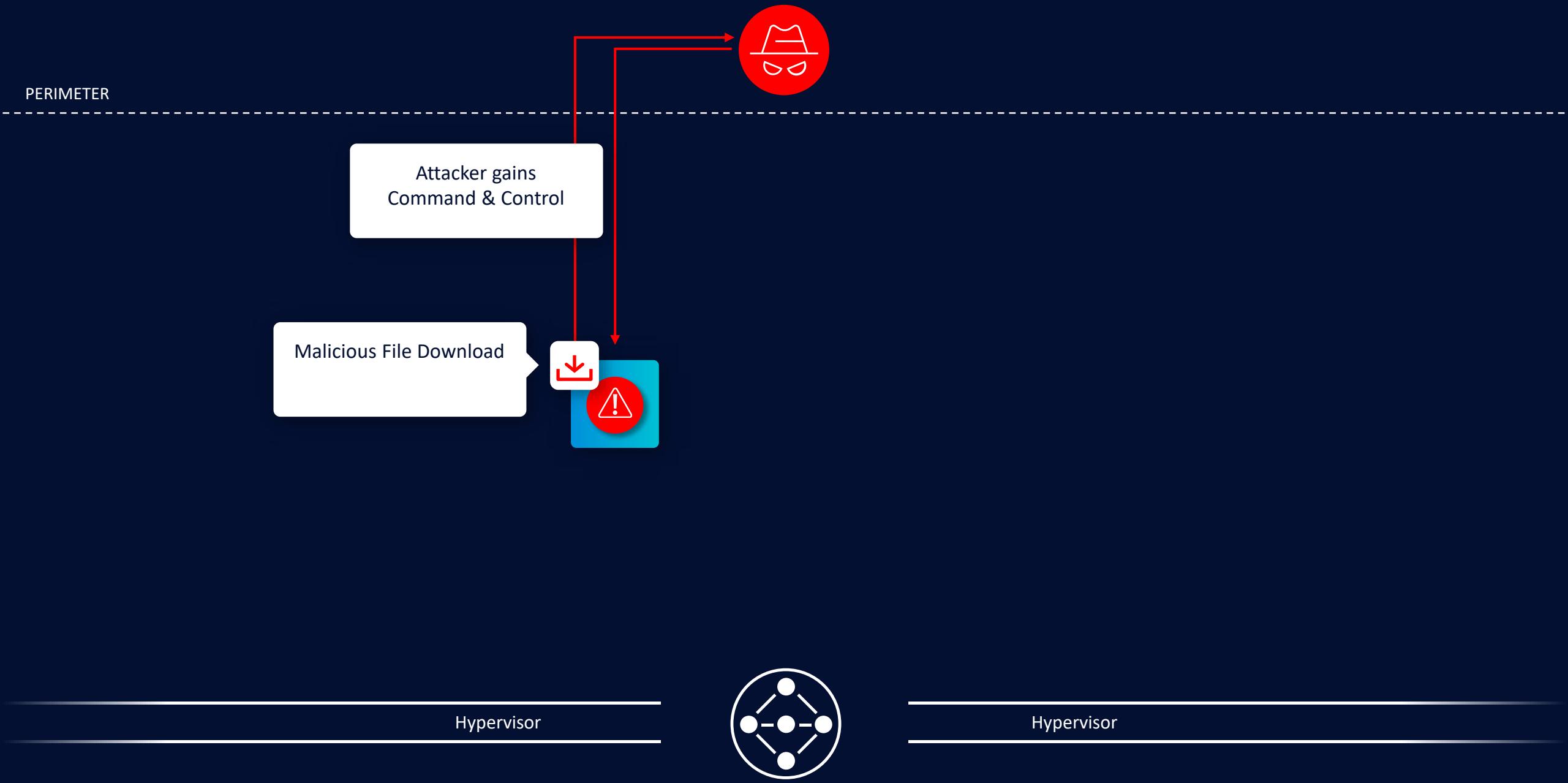
[2] Coveware Ransomware Marketplace Report

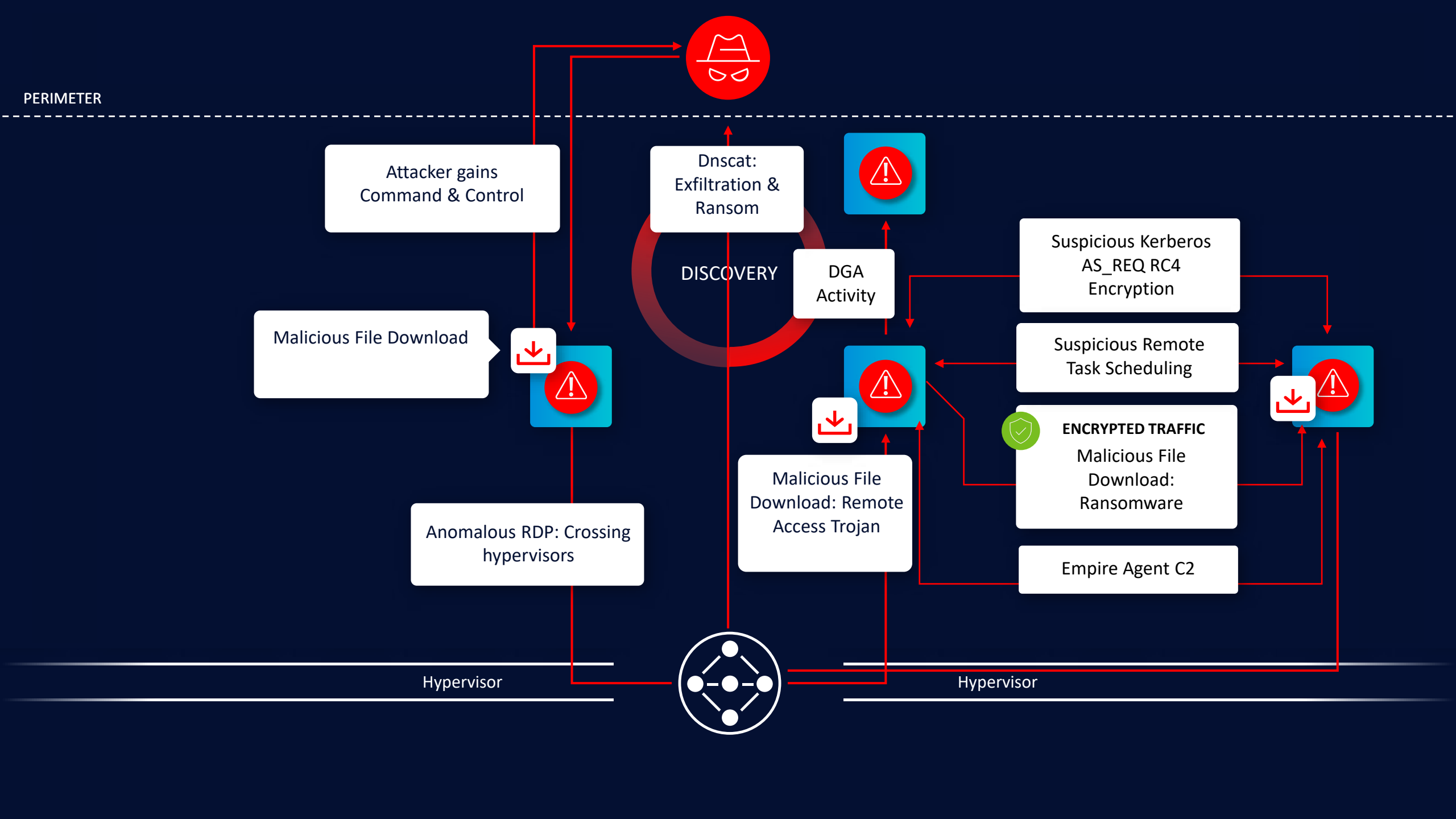
[3] Sophos State of Ransomware 2021

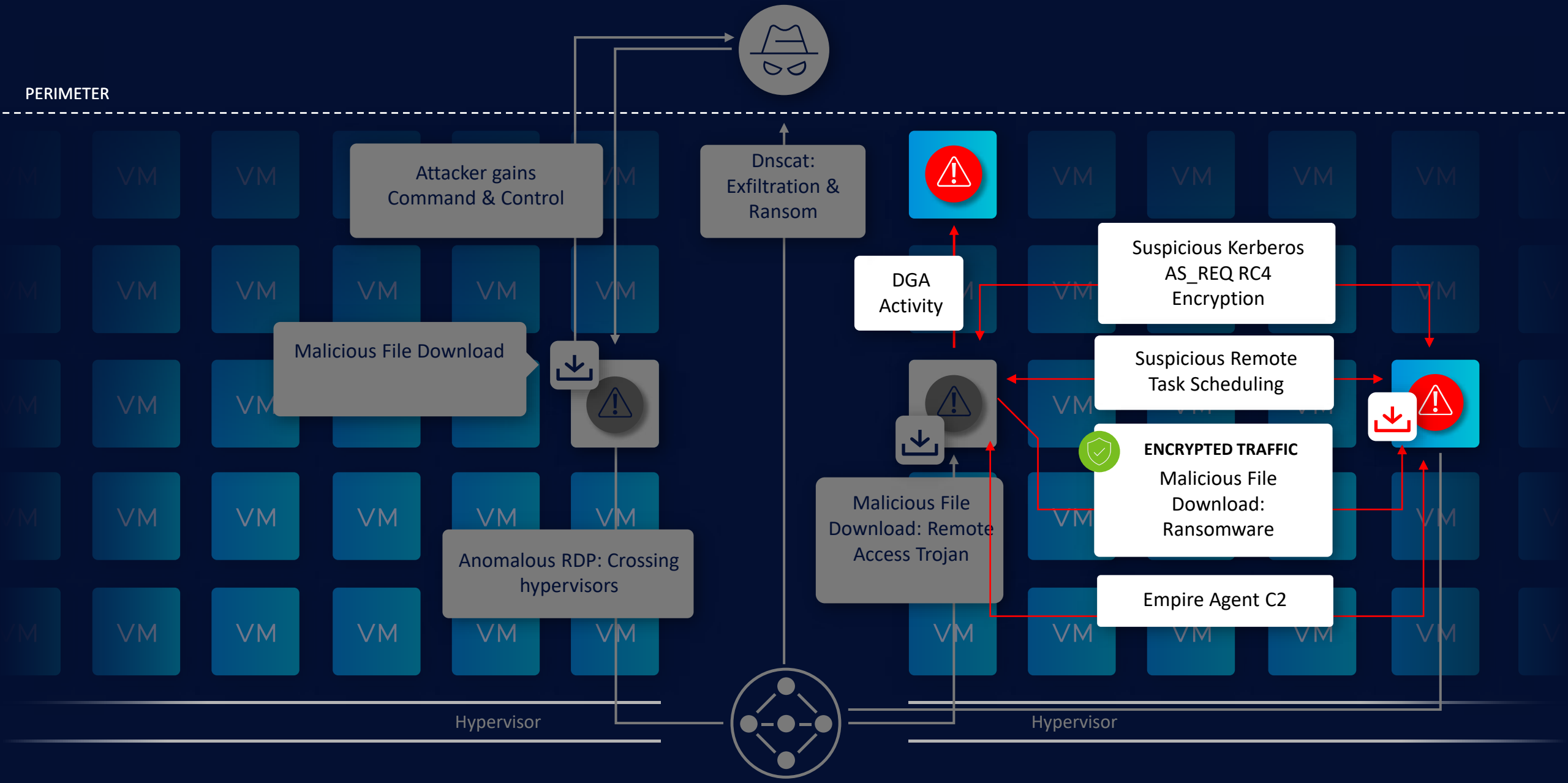
[4] IDC Market Forecast: WW Data Replication and Protection Software Forecast, 2022-2026

LATERAL MOVEMENT

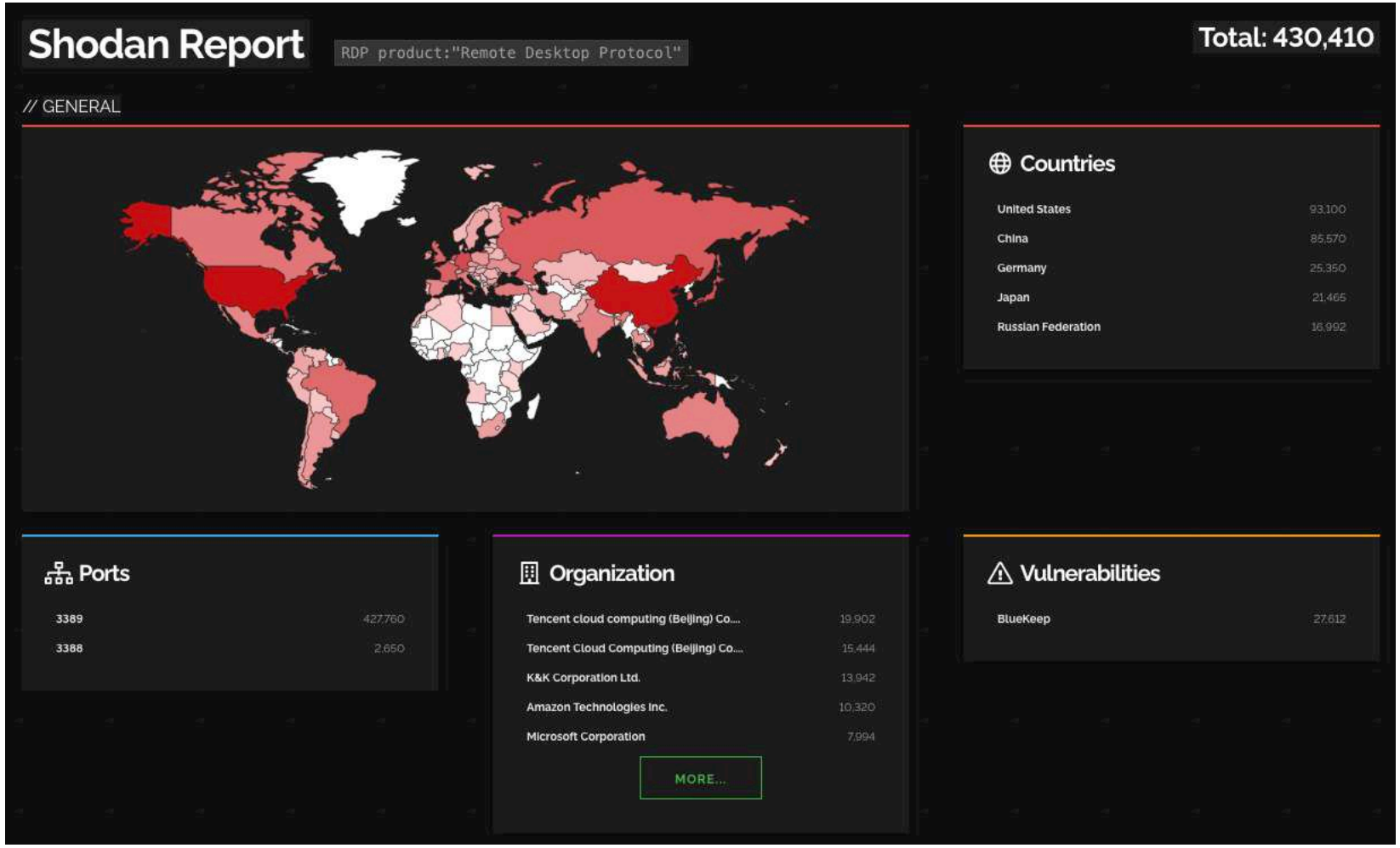
EXFILTRATION


PERIMETER
Attacker gains
Command & Control
Malicious File Download
Hypervisor
Hypervisor


PERIMETER
Attacker gains Command & Control
Dnscat: Exfiltration & Ransom
DISCOVERY
DGA Activity
Suspicious Kerberos AS_REQ RC4 Encryption
Malicious File Download
Suspicious Remote Task Scheduling
ENCRYPTED TRAFFIC
Malicious File Download: Ransomware
Malicious File Download: Remote Access Trojan
Anomalous RDP: Crossing hypervisors
Empire Agent C2
Hypervisor
Hypervisor

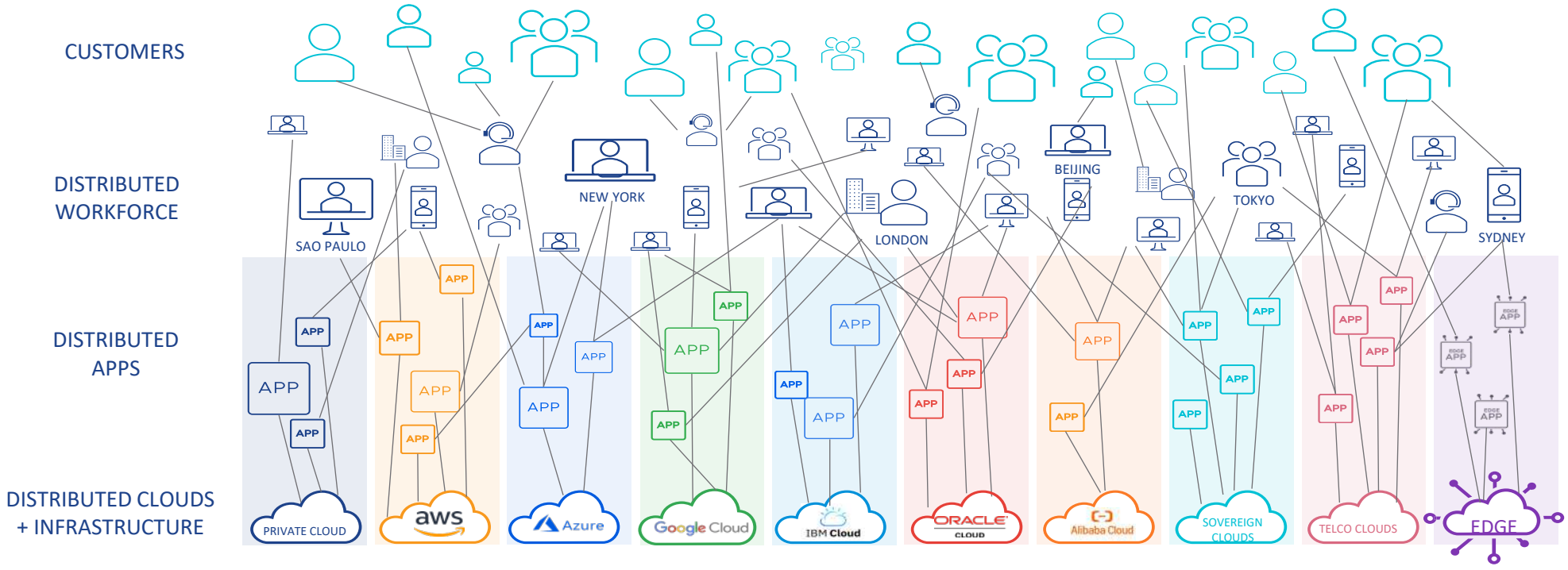

PERIMETER
Attacker gains Command & Control
Dnscat: Exfiltration & Ransom
DGA Activity
Suspicious Kerberos AS_REQ RC4 Encryption
Malicious File Download
Suspicious Remote Task Scheduling
ENCRYPTED TRAFFIC
Malicious File Download: Ransomware
Malicious File Download: Remote Access Trojan
Anomalous RDP: Crossing hypervisors
Empire Agent C2
Hypervisor
Hypervisor

RDP product:"Remote Desktop Protocol"



- 430,410 results for RDP
- More than 70% of lateral movement uses RDP
- Log4Shell vulnerability is also being targeted
- IDS/IPS can detect and protect against Log4shell attempts.
- Threat actors using Cobalt Strike (cracked) for Recon, and covert C2

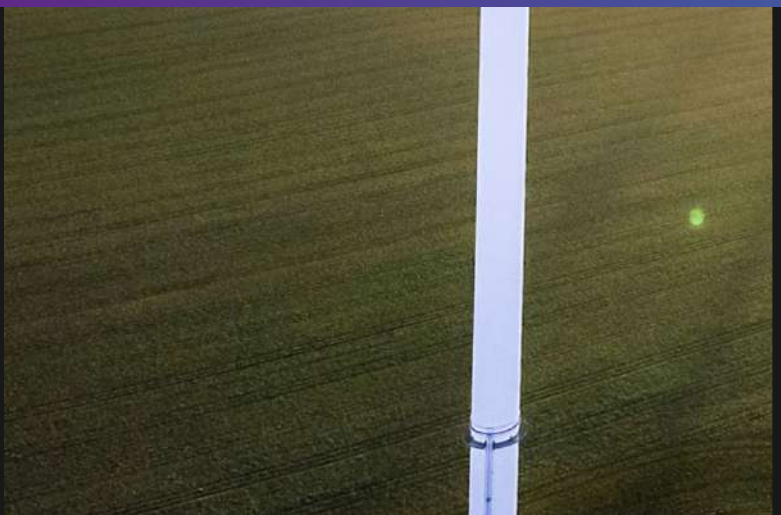
The new threat landscape requires a **distributed** approach to security.



20TB+

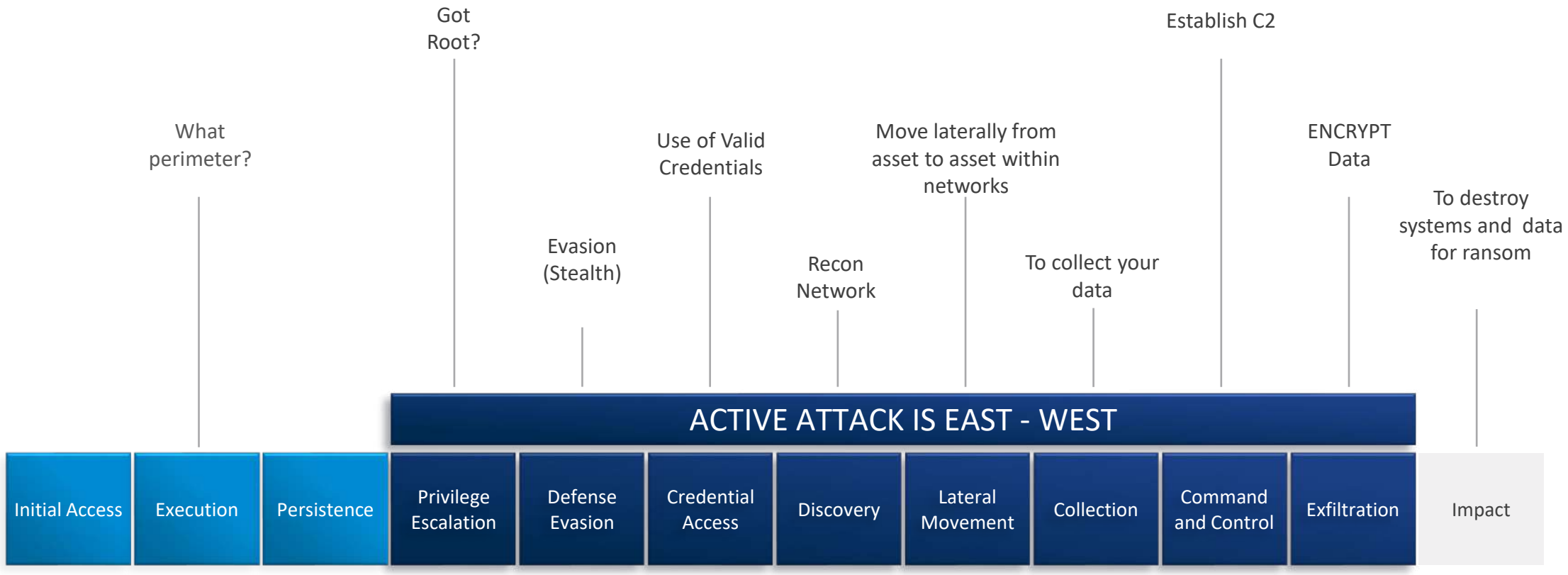
Internal Firewall for East-West Traffic

Lateral Security is the **New Battleground**



The New Battleground

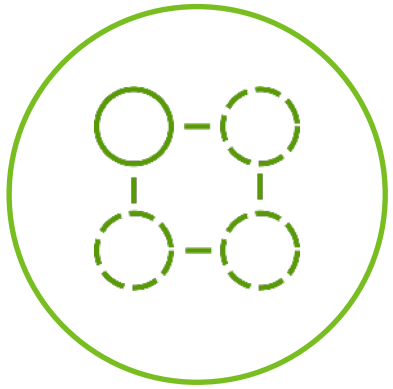
~~A day~~ *Many* days in the life of a breach (Back to Basics)



Obstacles Facing CISOs Today

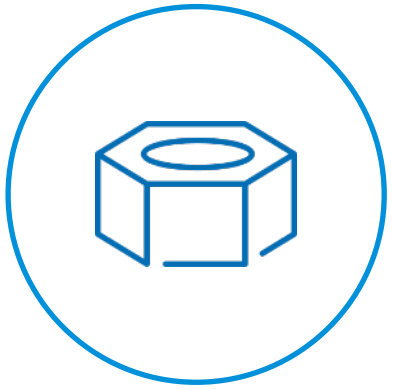
Security is…

Siloed



Threat-Centric

Bolted-on



Hard to Solve with Legacy Approaches

Siloed Teams

Minimal Collaboration Between:

- InfoSec
- Infrastructure
- Network
- Application

Too Many Tools

Driving:

- **Complexity**
- Misconfigurations
- Misalignments
- Integration Projects

Visibility Gaps

Lacking Visibility and Context for:

- Hardening
- Prevention
- Investigation
- **Response**

Detection Gaps

Missing Threats:

- Non-Malware
- New Ransomware
- **Lateral Movement**
- **Advanced Attacks**

How we solve this requires a new approach to security.

vmware®

CASE STUDY

35K+

employees

400+

apps

42

locations

VMware IT's Journey to Zero-Trust in Our Data Centers

Phase 1

- VDI segmentation
- VDI micro-segmentation
- 100+ apps micro-segmentation
- Perimeter inside perimeter

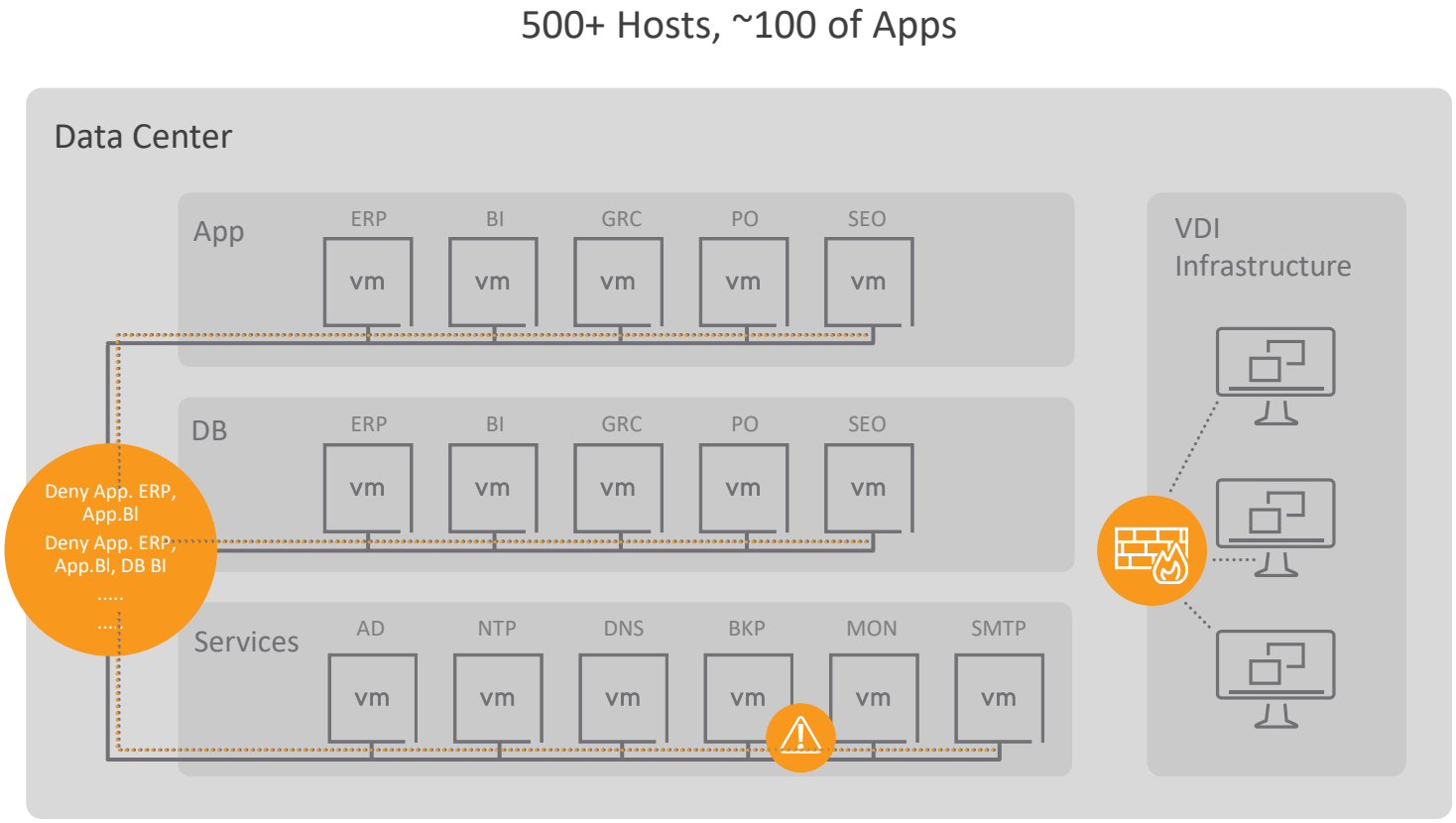
Phase 2

- Single-click deployment of IDS/IPS for east-west traffic
- Deploying Network Detection and Response

Phase 3

- Identity-based internal firewalling (AD user)
- No tap Network Traffic Analysis

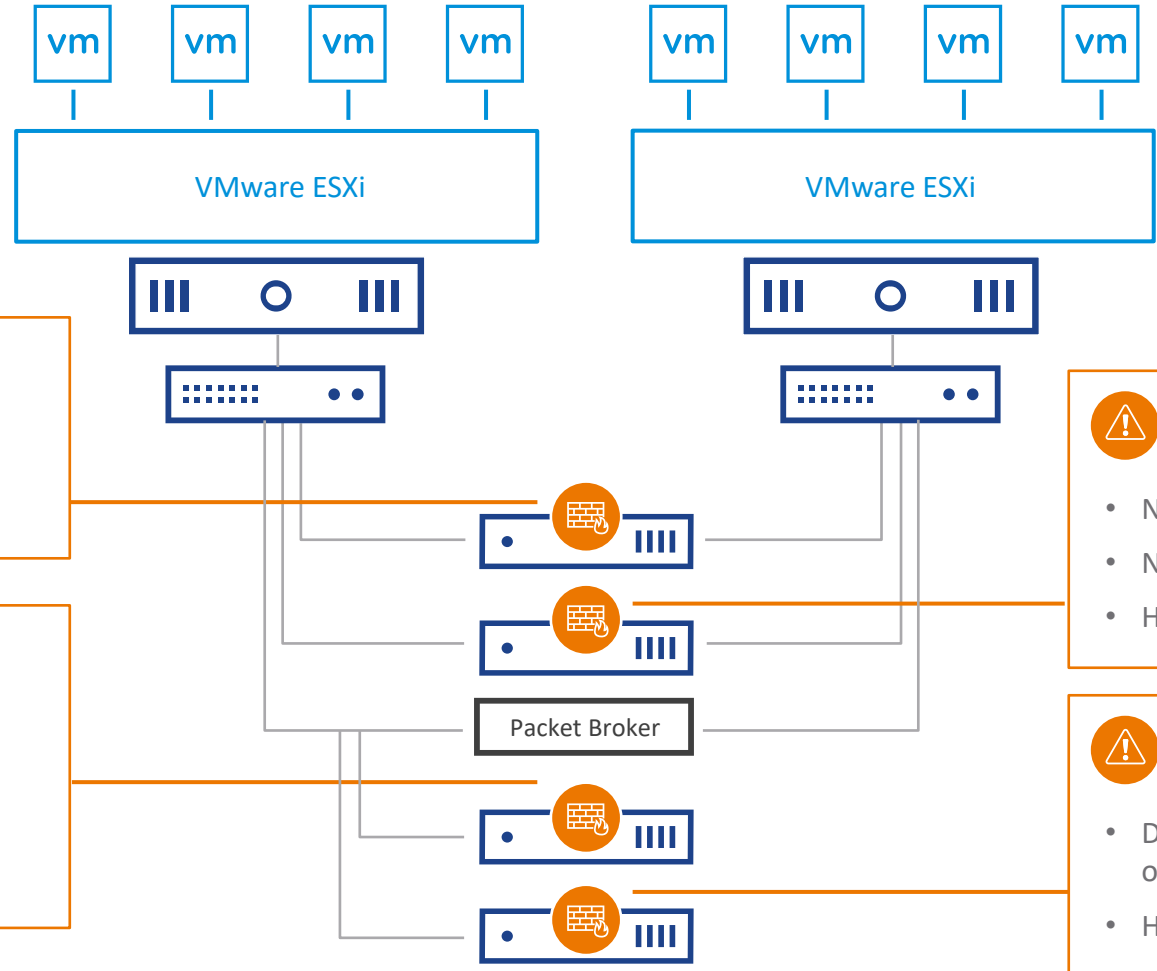
Security Challenges in the Data Center



- Critical applications were lying wide open internally
- Securing with traditional firewalls was creating choke points
- Isolating VDI desktops with traditional firewalls was not practical and required complex hair-pinning
- Lack of dynamic policies was resulting in shadow and stale policies, and massive rule bloat

Network Security Controls and Threat Protection

VMware Legacy



Network-Based Firewalling

- Manual and labor-intensive
- IP/Subnet based

Network Sandbox

- Detection technology easily bypassed by evasive malware
- Fails to detect advanced threats

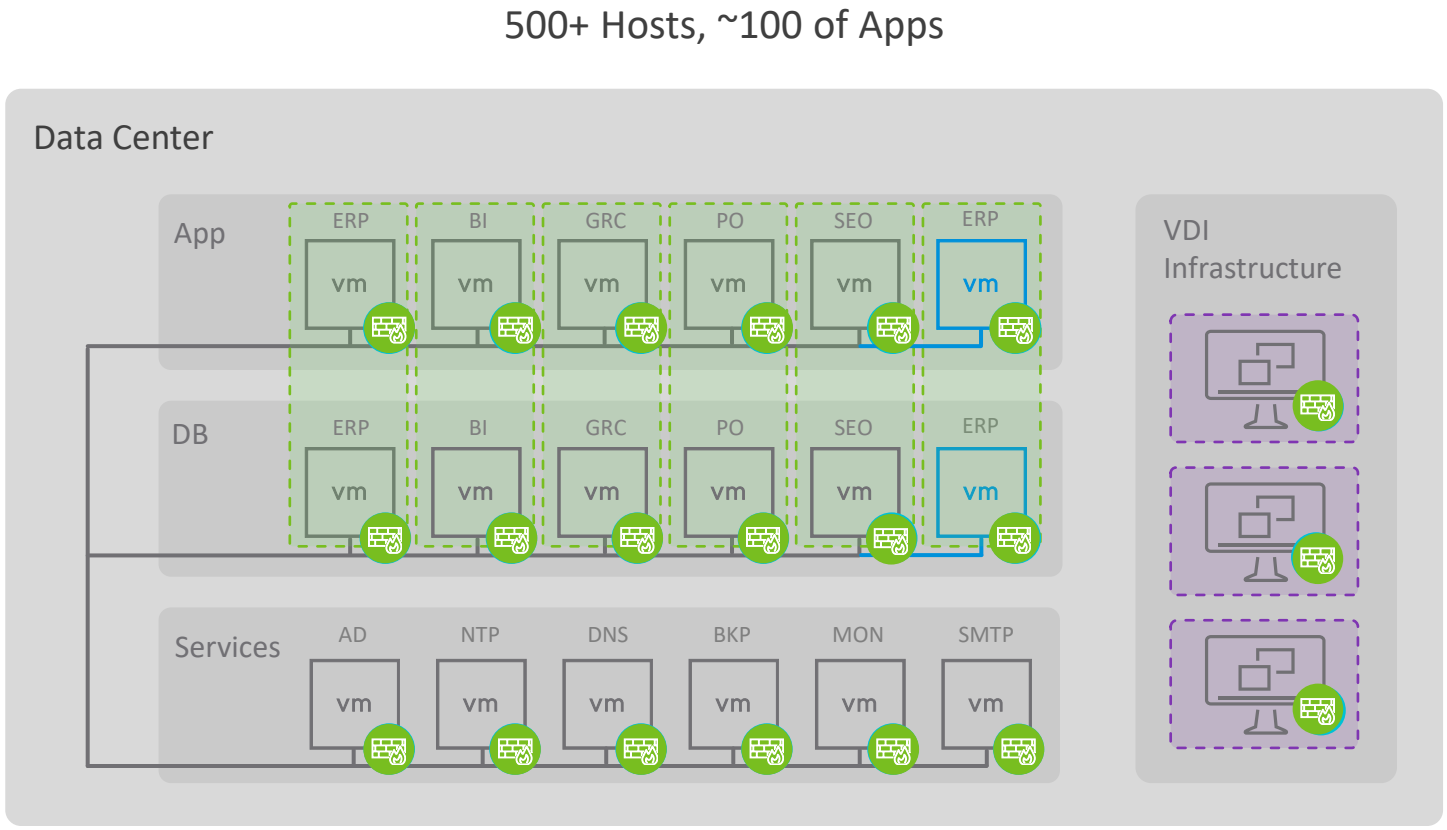
IDS/IPS

- No Environmental Context
- No East/West Visibility
- High false positive rate

Network Traffic Analysis

- Difficult and costly to hairpin 100% of traffic
- High false positive rates

Using NSX Firewall for Segmentation with Automated Policy

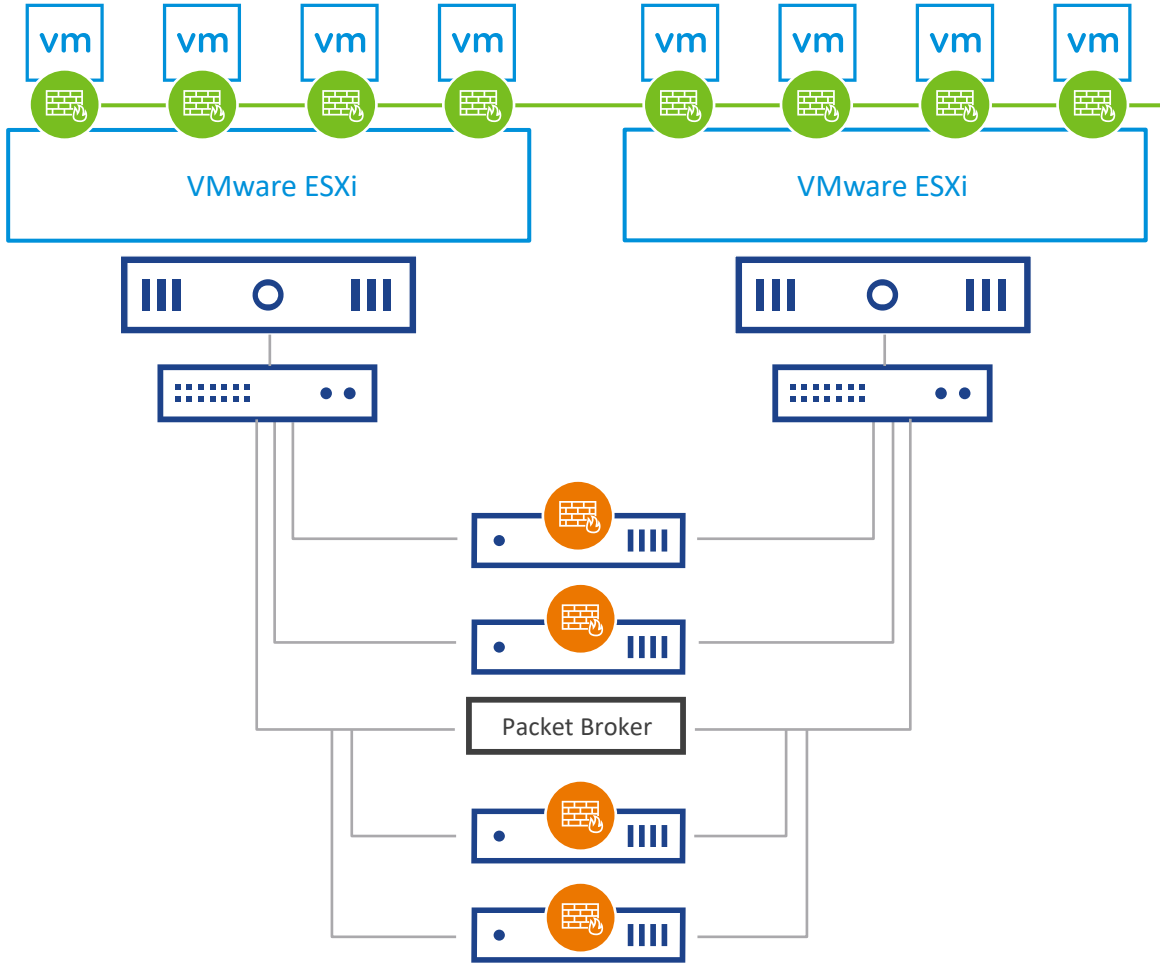


Solution

1. Visibility: Created application maps and discovery policies
2. Micro-segmentation: Granularly segmented ~100 critical applications e.g. SAP
3. Secure VDI: Isolated virtual user desktops with single line of policy
4. Automation: Additional workloads automatically segmented using dynamic security policies

Network Security Controls and Threat Protection

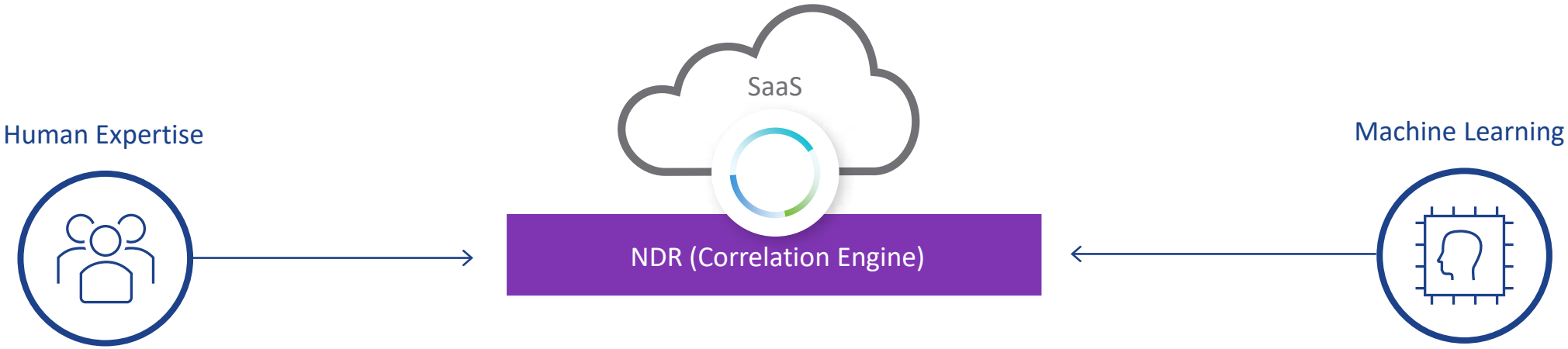
NSX Multi-Cloud Security

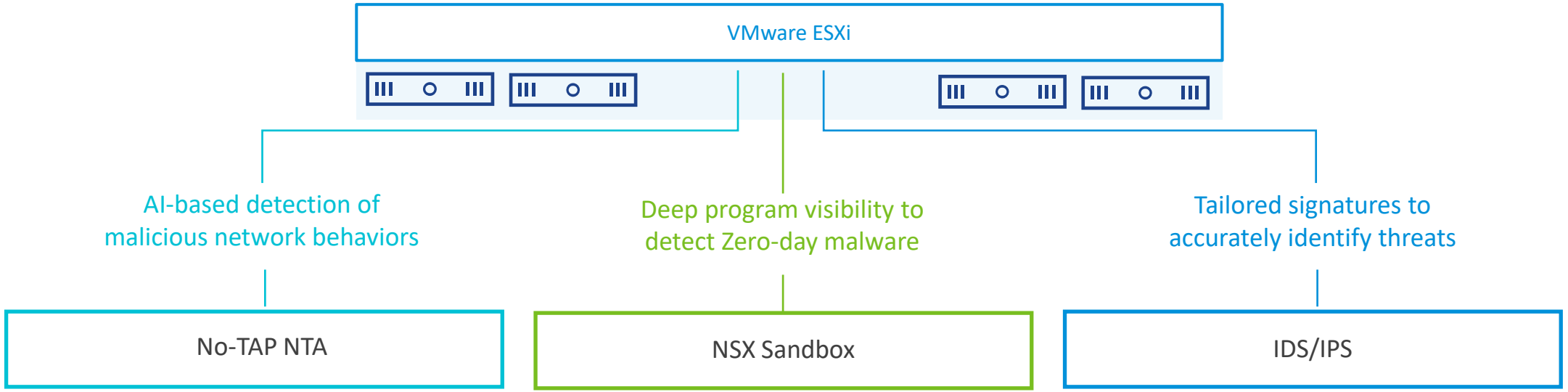


VMware NSX Firewall
Hypervisor Based Advanced Threat Protection

- No Network Changes
- Hypervisor Observability
- Segmentation/ Micro-segmentation
- NSX Network Detection & Response
  - No-Tap NTA (E-W Visibility)
  - NSX Sandbox (Guest Introspection)
  - NSX Distributed IDS/IPS
  - Network Event Correlation

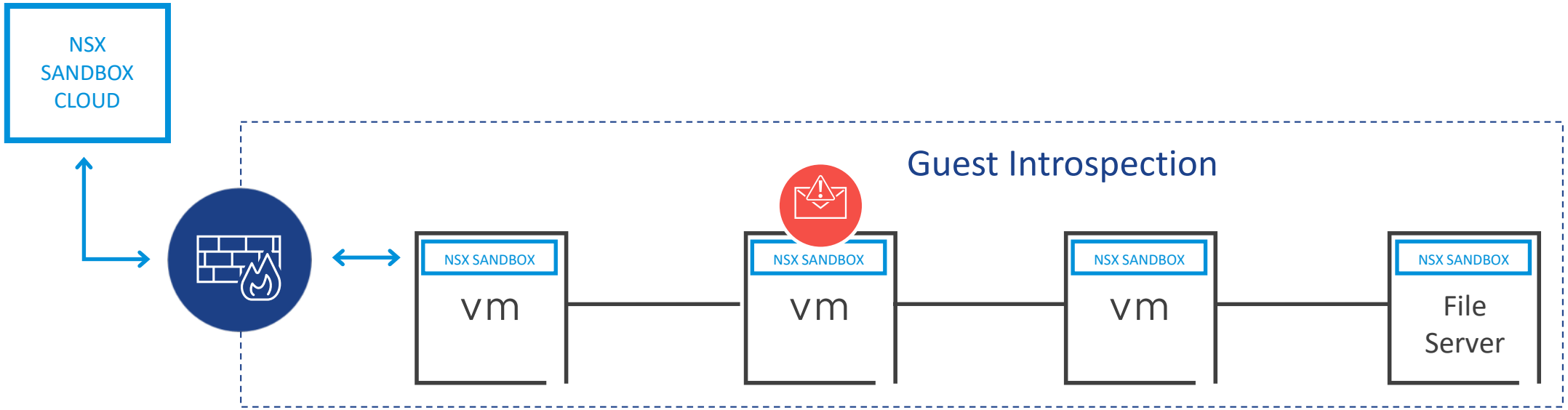
NSX Network Detection & Response (NDR)





NSX Sandbox

Sandbox
IDS/IPS
NTA



NSX Sandbox

Sandbox
IDS/IPS
NTA

Full System Emulation

Ability to see advanced evasive techniques from malware

Behavior Appears Harmless

Understand detailed ransomware activity

Read Running Processes

[redacted]

[redacted]

Encrypt Files using Ransomware Routine

[redacted]

Open Network Connection to Remote Site

Send Encryption Key to C&C Server

...

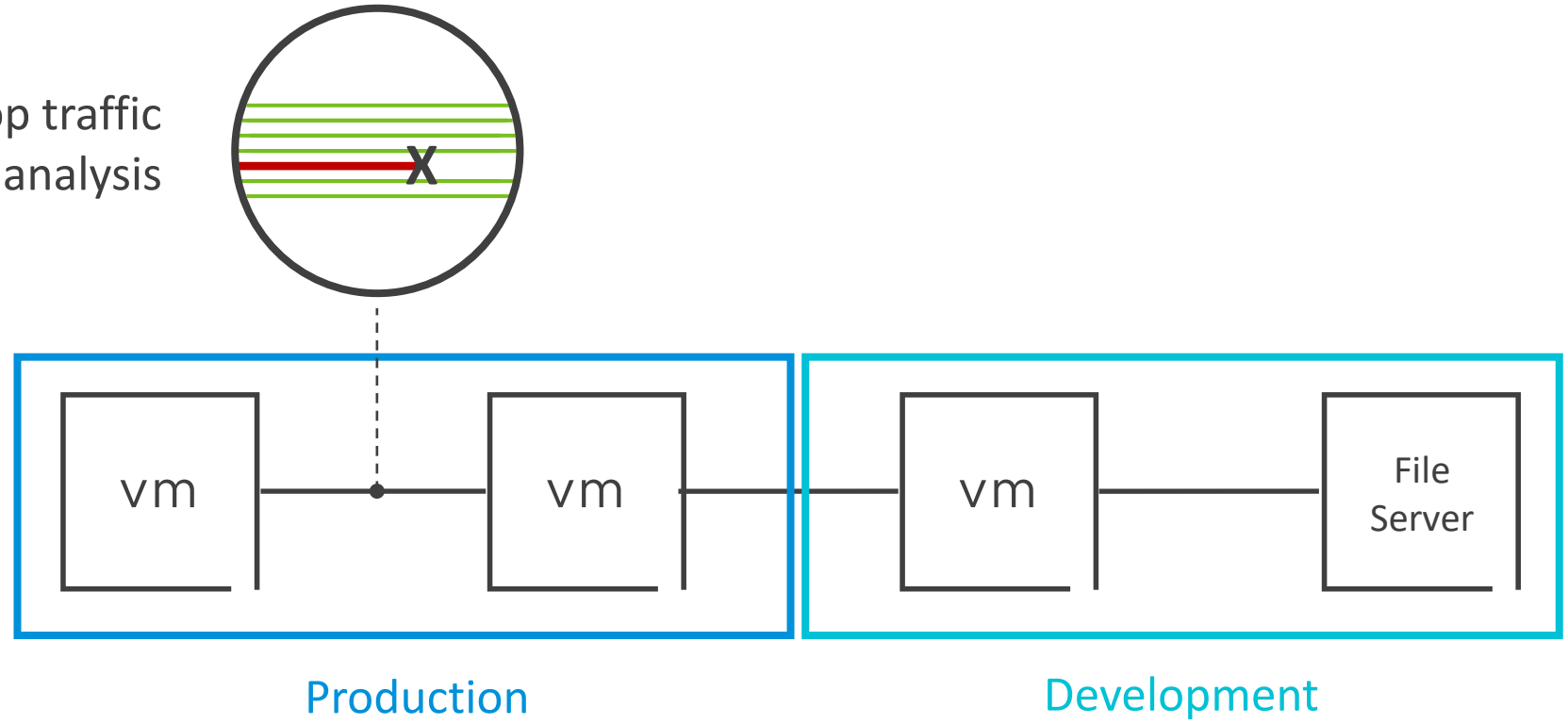
[redacted]

NSX SANDBOX

File Server

NSX Distributed IDS/IPS

Per hop traffic analysis



Signature-Based Detection at Every Hop

Sandbox
IDS/IPS
NTA

Finance_app IDPS

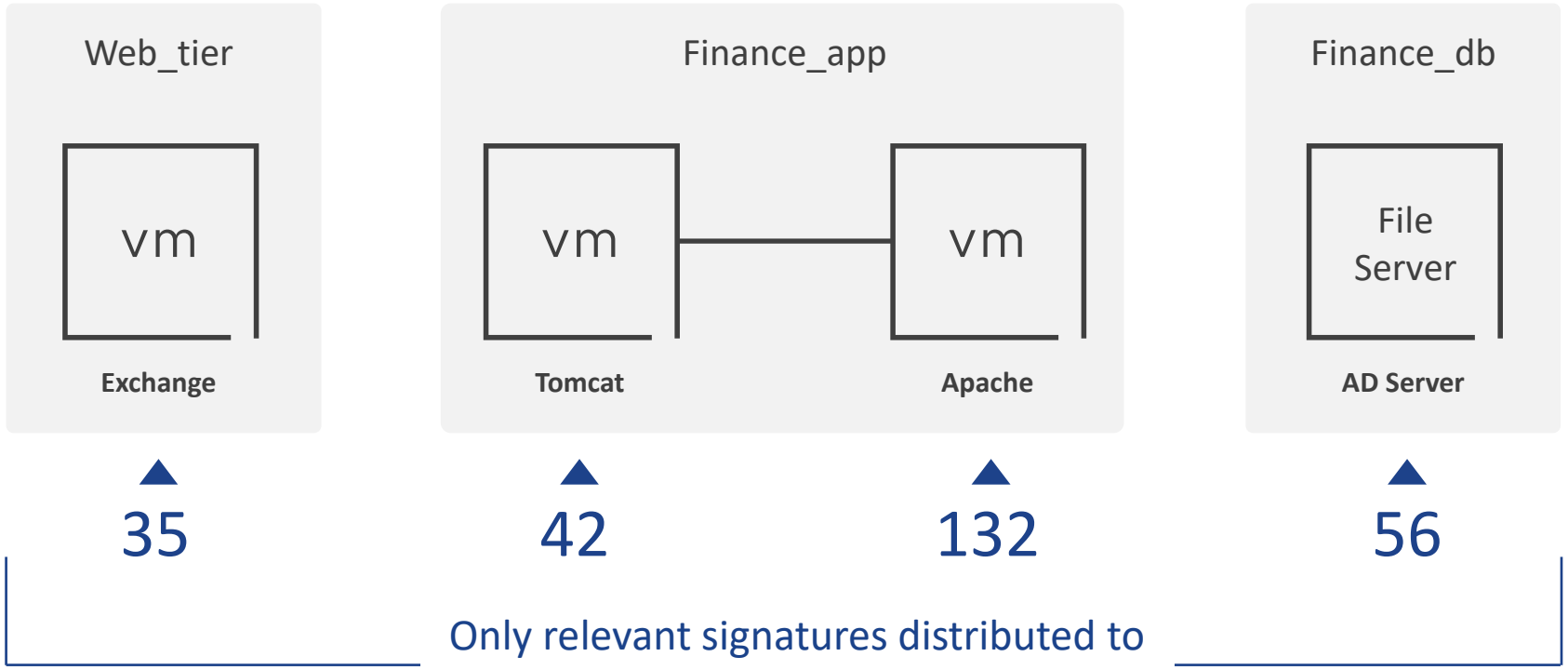
Apache IDS/IPS

MySQL IDS/IPS

…to drop insignificant signatures.

From ~13k signatures evaluated at each IDPS engine.

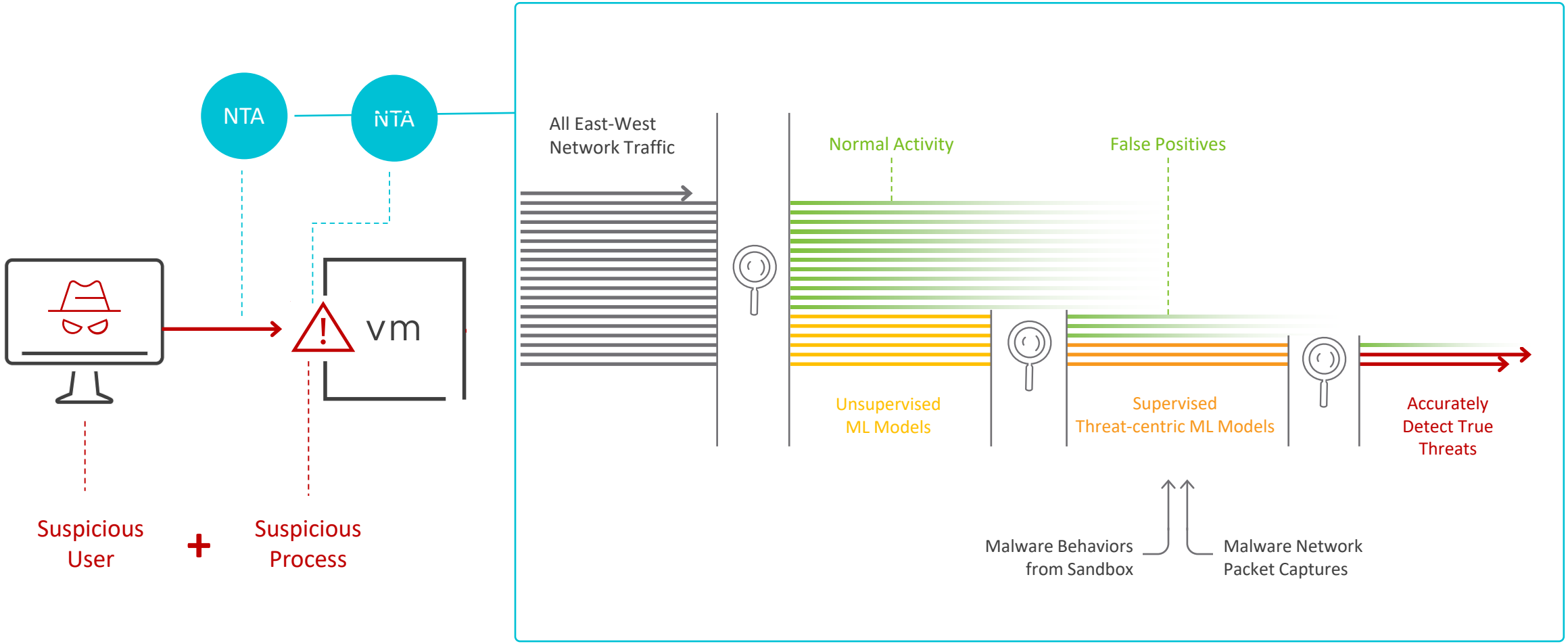
>80%*



* Numbers are not accurate, for illustrative purpose only

Network Traffic Analysis

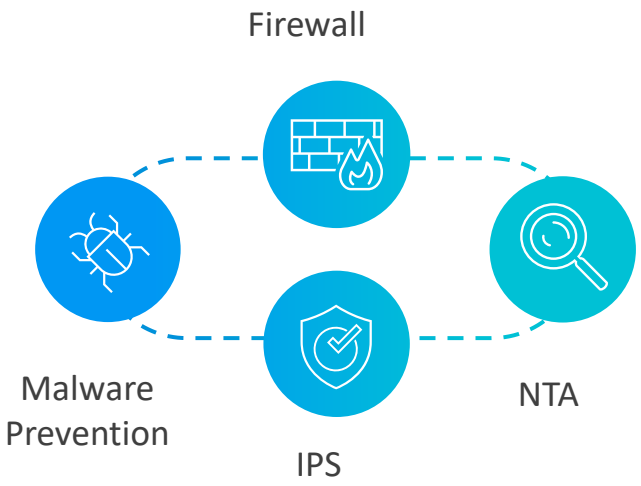
Sandbox
IDS/IPS
NTA



MITRE ATT&CK™

Tactics and Techniques

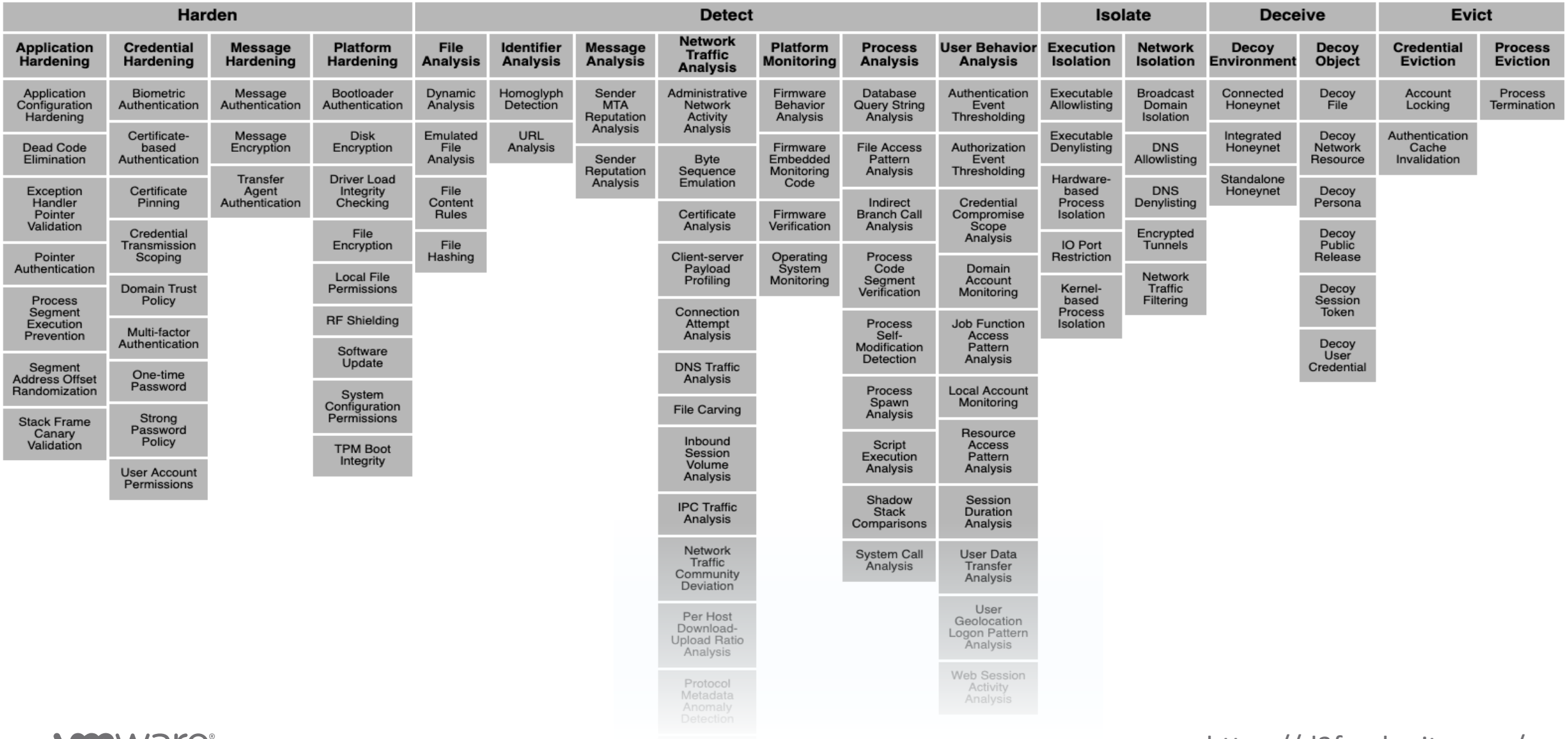
VMware
NSX Firewall



ATT&CK TACTICS

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE D3FEND™



https://d3fend.mitre.org/

The Impact Thus Far

500
Gbps traffic Secured

Better Security

- Security throughput scales with workloads
- Zero Trust architecture prevents lateral movement between apps

90%
Reduction in Security Policies

Operational Agility

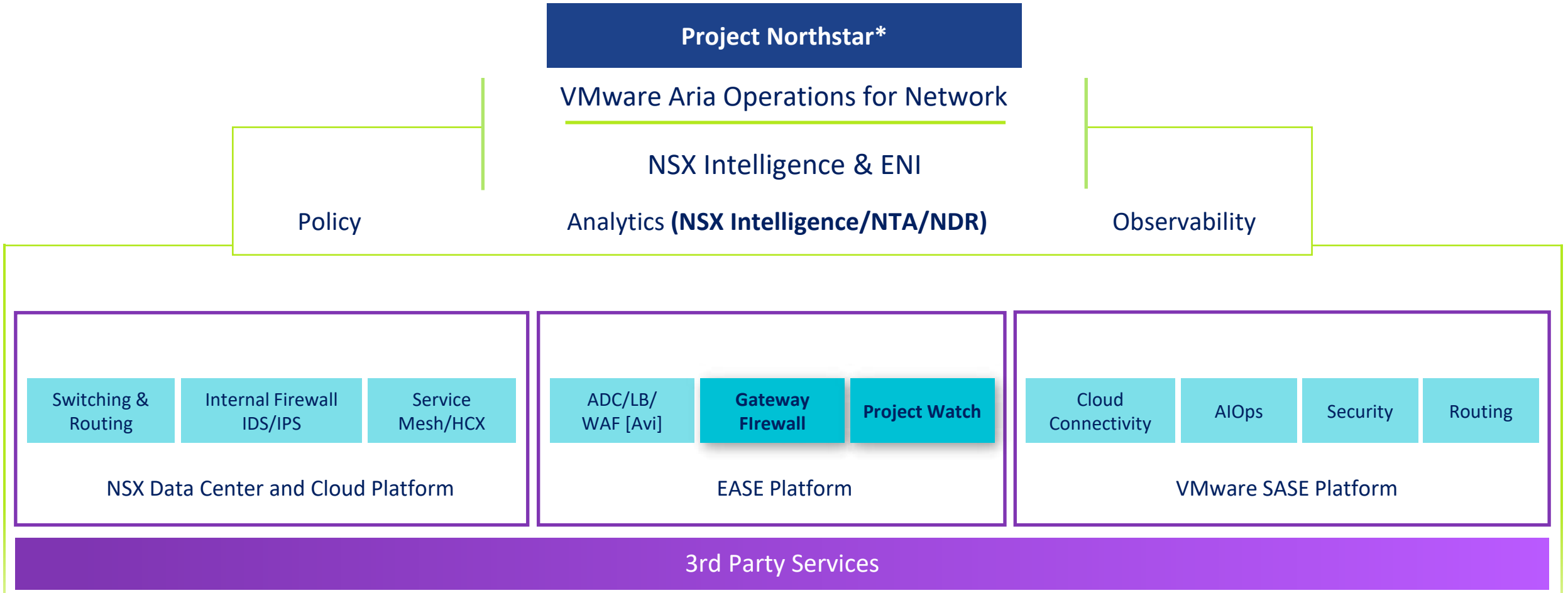
- Concise Security Groups replace IP/Port/Protocol based polices
- Policy automation with app life cycle eliminates stale policies

40
hrs/month maintenance savings

Cost Savings

- New workloads automatically inherit existing policies
- No need for network changes when adding new applications

Visibility & Enforcement across the Attack Chain



* Project Northstar announced at Vmware Explore, currently Tech Preview

30K+

VMware Security Customers

#

SD
Ve

SE Labs

SE Labs Breach Response Detection Test

VMware NSX Network Detection and Response

August 2021

RATINGS

SE Labs AAA Network Detection & Response AUGUST 2021

Total Rating	100%
Detection Accuracy	100%
Legitimate Accuracy	100%

LEGITIMATE ACCURACY

False Positives	0%

THREAT RESPONSE DETAILS

Threat	Target	Score	Overall Score
FIN7 & Carbanak		100%	100%
OilRig		100%	
APT3		100%	
APT29		100%	

This is a summary of the full test report available selabs.uk/vmware.

Detection scores represent the product's behaviour when encountering network-specific threat techniques.

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity. We support businesses that are researching, buying and deploying security solutions. We are able to test a wide range of products and services using cutting edge testing methodologies that lead the security testing industry. SE Labs focusses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Licensed for republication by VMware, Inc

FORRESTER®
WAVE LEADER 2021
Endpoint Security Software As A Service

FORRESTER®
NEW WAVE LEADER 2021
Zero Trust Network Access
3

Leader
Gartner
2022 Magic Quadrant™ for WAN Edge Infrastructure
4

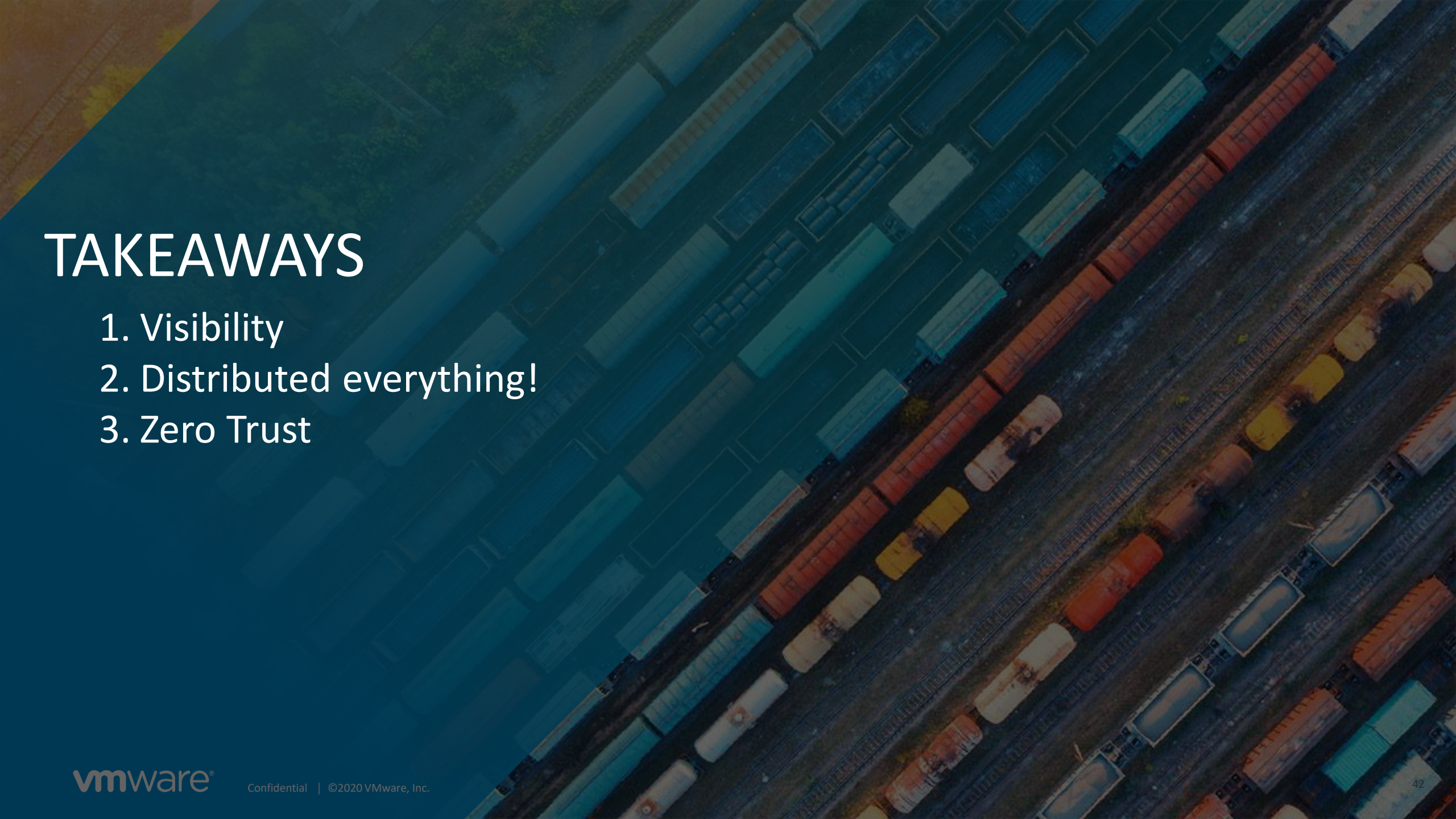
SE Labs AAA Network Detection & Response AUGUST 2021

VMware NSX Network Detection and Response

1 VMware Internal Analysis, August 2022;
2 Forrester Research. (2022). (rep.). *The Forrester Ne*
3 Forrester Research. (2022). (rep.). *The Forrester Wa*
4 Gartner. (2020). (rep.) *Gartner Magic Quadrant for*
5 SE Labs. (2022). (rep.) *Network Detection & Respon*
6 VMware is 1 of 5 enterprise firewall vendors (with greater than $500M in annual revenue) in the Forrester Now Tech: Enterprise Firewalls, Q1 2020

TAKEAWAYS

1. Visibility
2. Distributed everything!
3. Zero Trust



Thank You