Threat Investigation

with VMware ATP

vmware by Broadcom

Why you should be concerned about Lateral Security ?

Today's Security Realities

Operational Inefficiencies and Unmitigated Risks

Lack of Visibility

Across Environments

Lack of Communication

Between Roles and Orgs

Operational Inefficiency

Unmitigated Risk

Lack of Automation

Across tool/platforms

In Policies and Events

Lack of Context

Today's Security Realities

Freedom of Movement

44%

of breaches reported lateral movement[1]

204

Days to detect a breach[2]

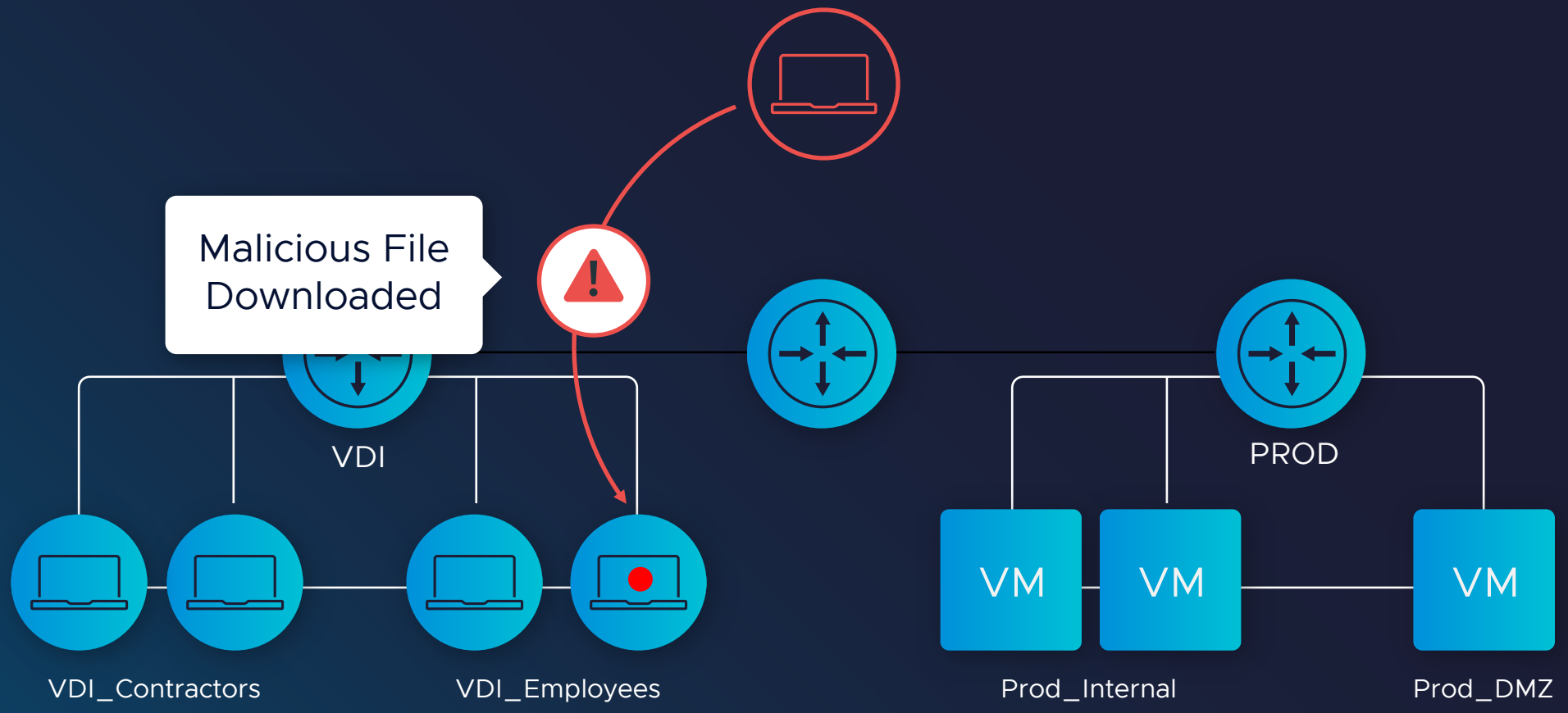
$4.35M

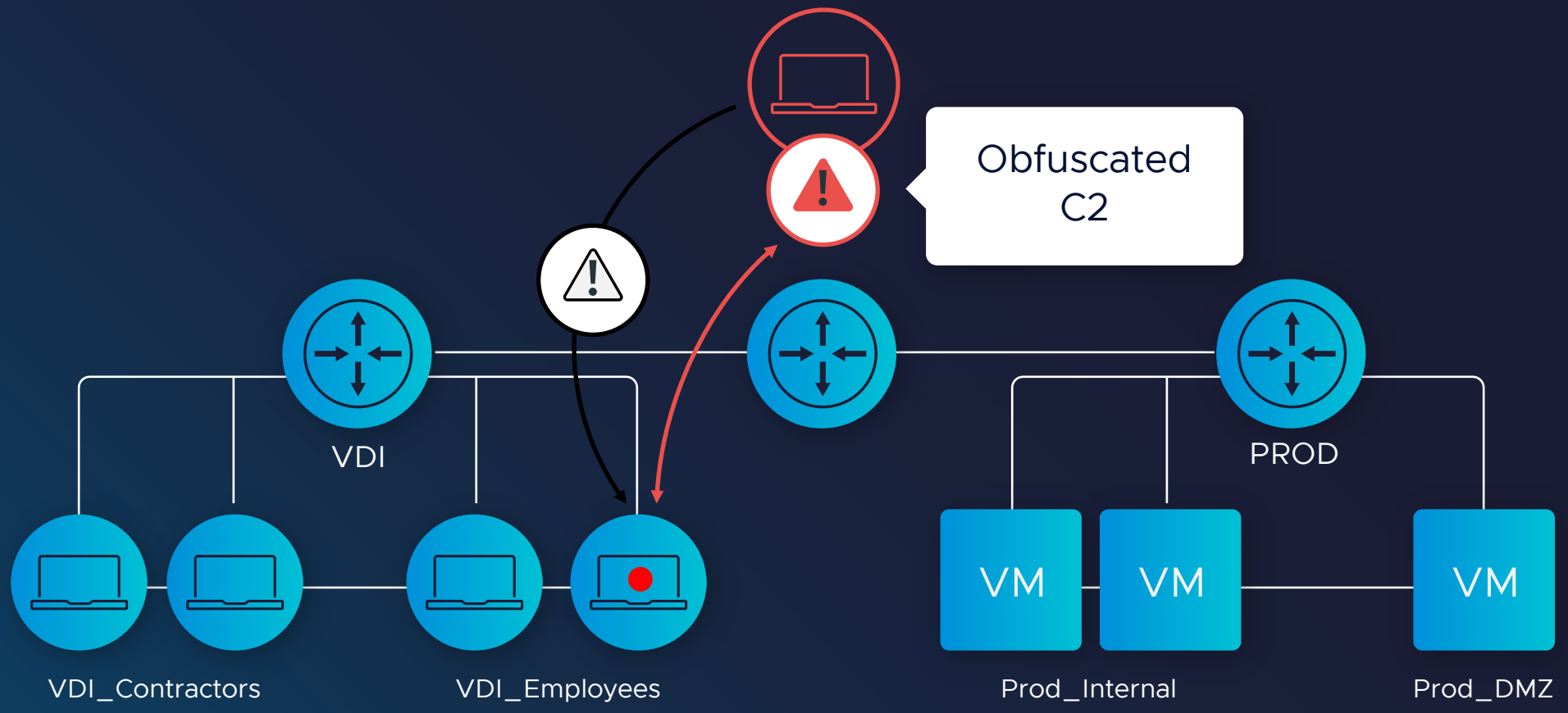
Average cost of a data breach[3]

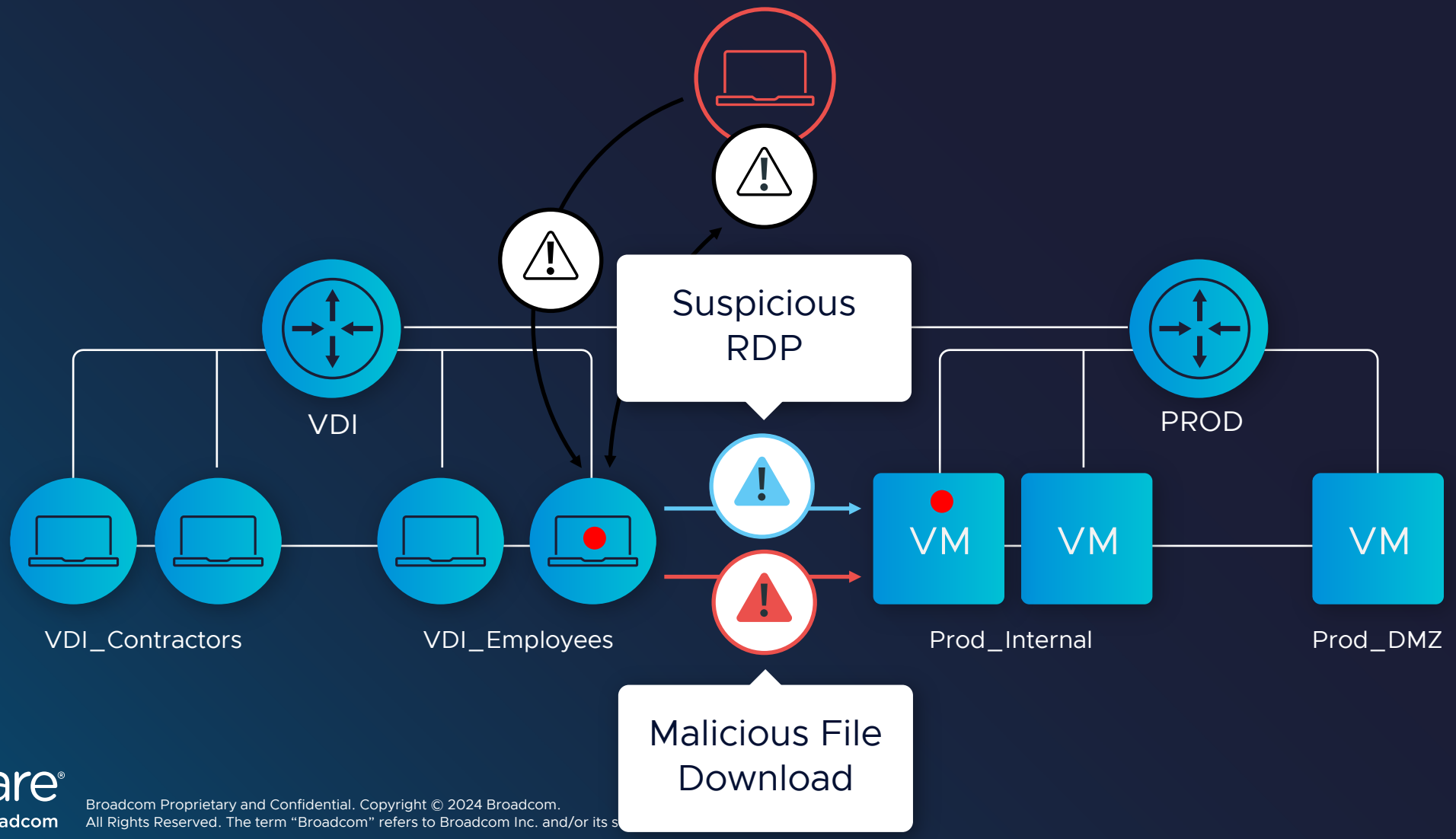
Source 1 – 2022 VMware Global Threat Report, Source 2 - 2023 Verizon Data Breach Investigation report, 3 – 2023 IBM Cost of Data Breach Report

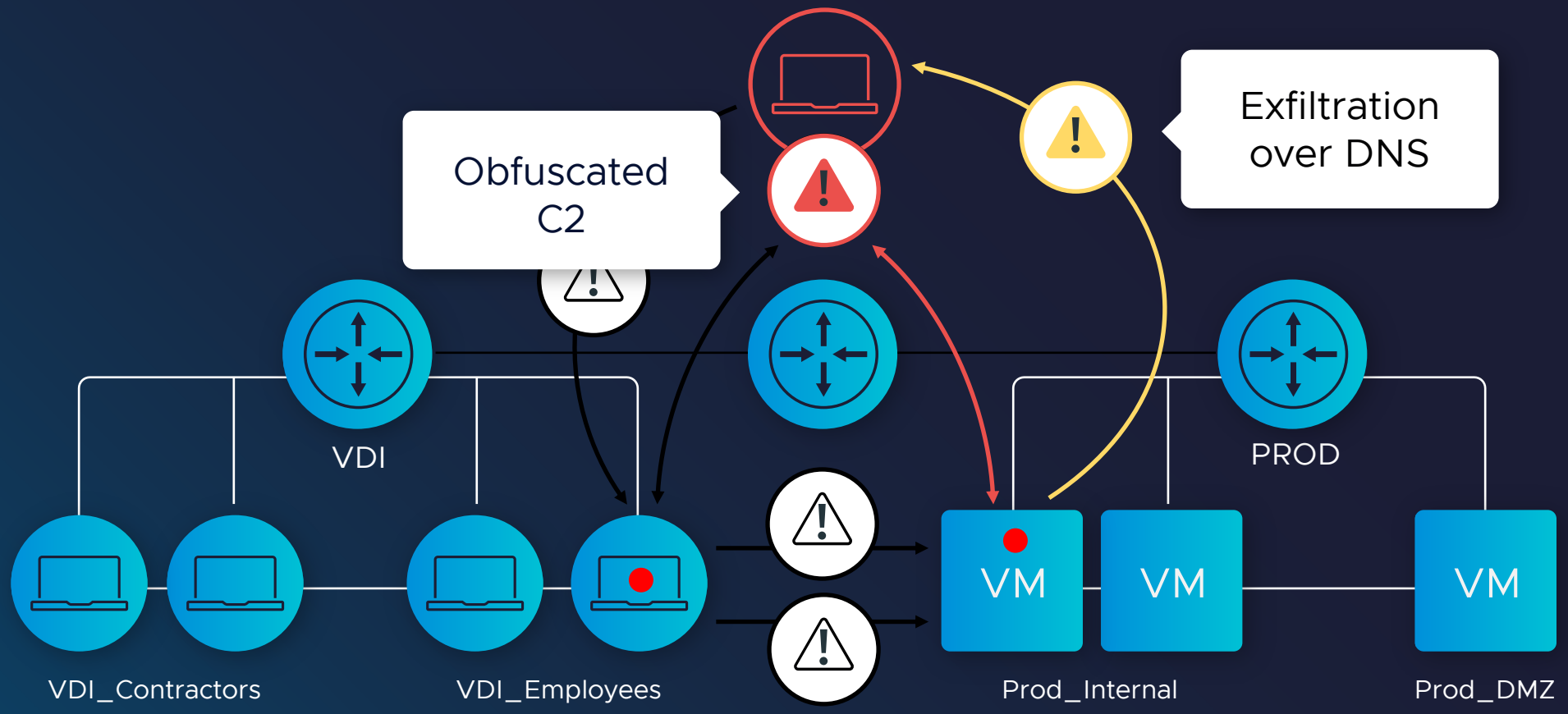
Today's Security Realities

You cannot protect what you cannot see



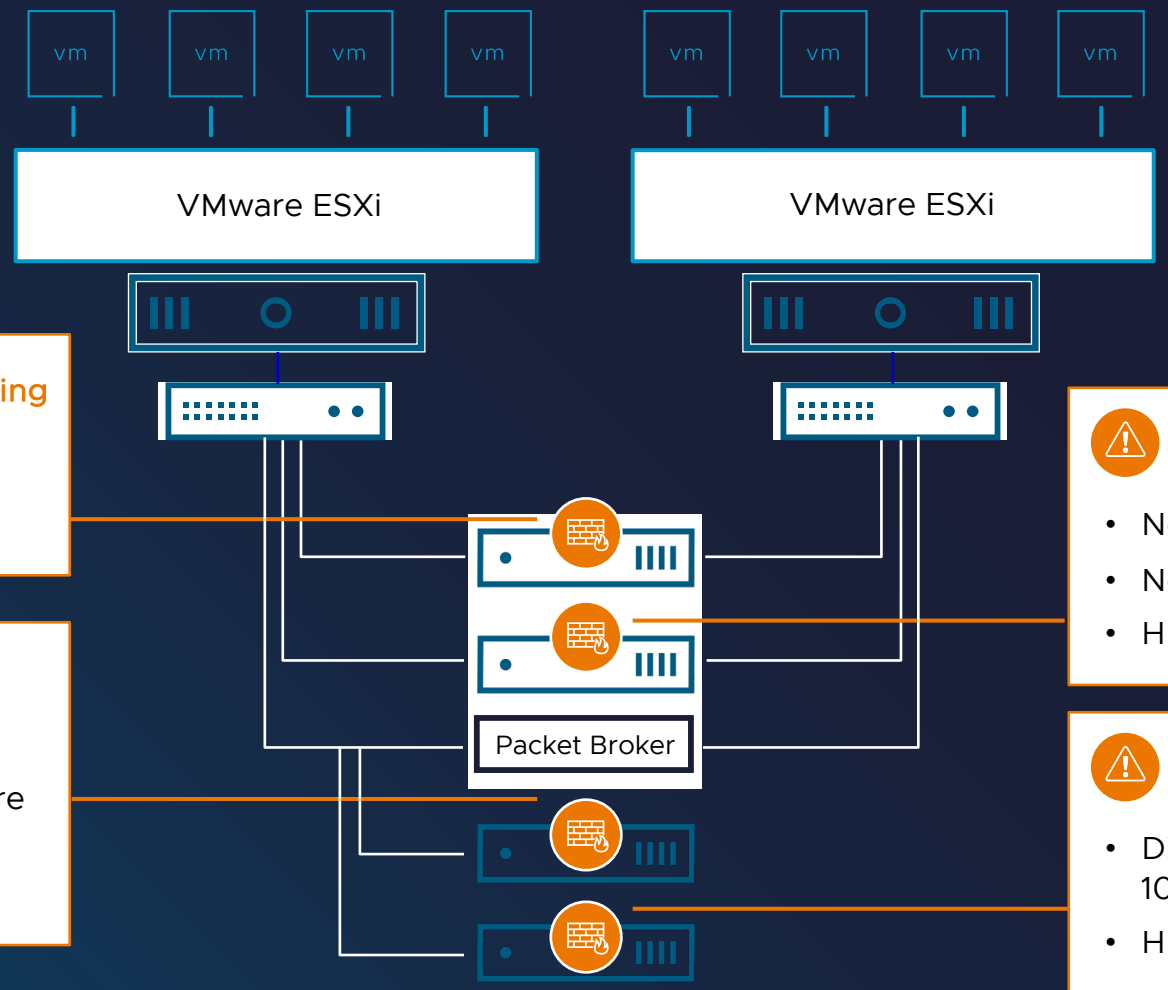






Today's Security Realities

Legacy Solutions



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

Turning on the Lights

With VMware Security Intelligence and ATP

vmware by Broadcom

Turning on the Lights

Comprehensive VMware Lateral Security Defense

Threat Analytics Powered by AI

VMware Lateral Security

Security Intelligence
Visibility | Micro-Segmentation Planning

App Discovery
Security Analytics
Rule Recommendations

Advanced Threat Prevention
IDS/IPS | NTA | NDR | Sandbox

Zero-day Exploits
Known Vulnerabilities
Anomaly Detection

Distributed Firewall

Gateway Firewall

Micro Segmentation
Segment Zones

Turning on the Lights

Comprehensive VMware Lateral Security Defense

Threat Analytics Powered by AI

VMware Lateral Security

Security Intelligence
Visibility | Micro-Segmentation Planning

App Discovery
Security Analytics
Rule Recommendations

Advanced Threat Prevention
IDS/IPS | NTA | NDR | Sandbox

Zero-day Exploits
Known Vulnerabilities
Anomaly Detection

Distributed Firewall

Gateway Firewall

Micro Segmentation
Segment Zones

Today's Security Realities

You cannot protect what you cannot see

1. How many applications are communicating with each other on the network?
2. What micro-segmentation policies need to be created?
3. Are these communications normal or abnormal?
4. Which of the thousands of alerts are real security attacks?

Data Center Network hosts thousands of application components

It is a black box for most Network Security teams

VMware Security Intelligence

Real-Time Flow Visibility, Network Traffic Analysis and Firewall Planning

Security Intelligence Data Platform

Security Intelligence Visualization

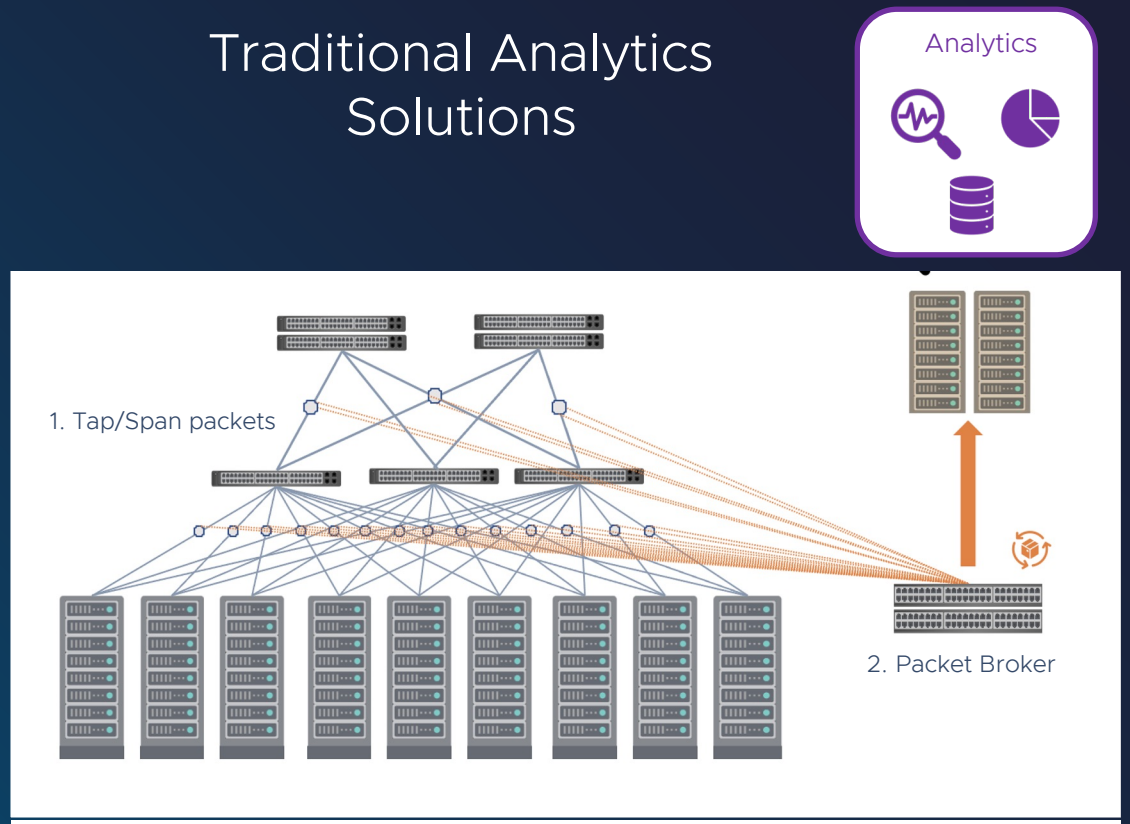
Security Intelligence Security Policy Recommendations

Security Intelligence Network Traffic Analysis

VMware Security Intelligence

Bolted-on versus Built-in Model for Analytics

Traditional Analytics Solutions

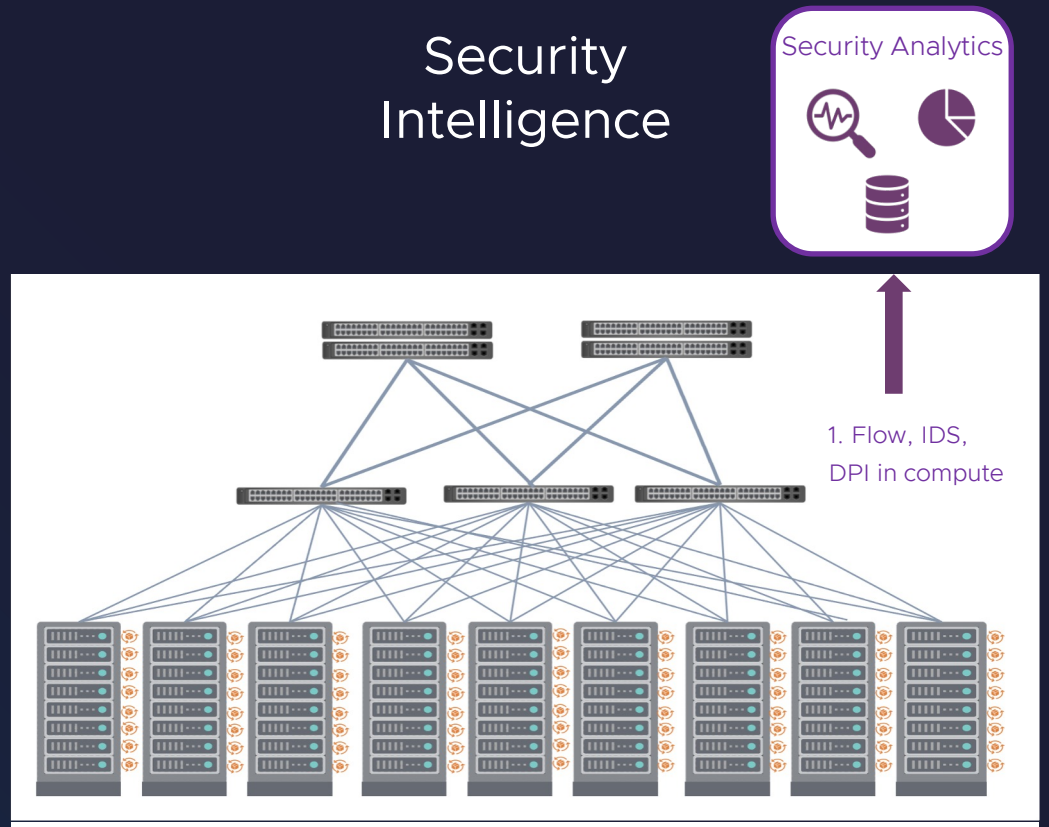


Duplicate/Mirror traffic to Analytics solutions

High Capex and Opex implications

Limited coverage due to performance and cost implications

Security Intelligence



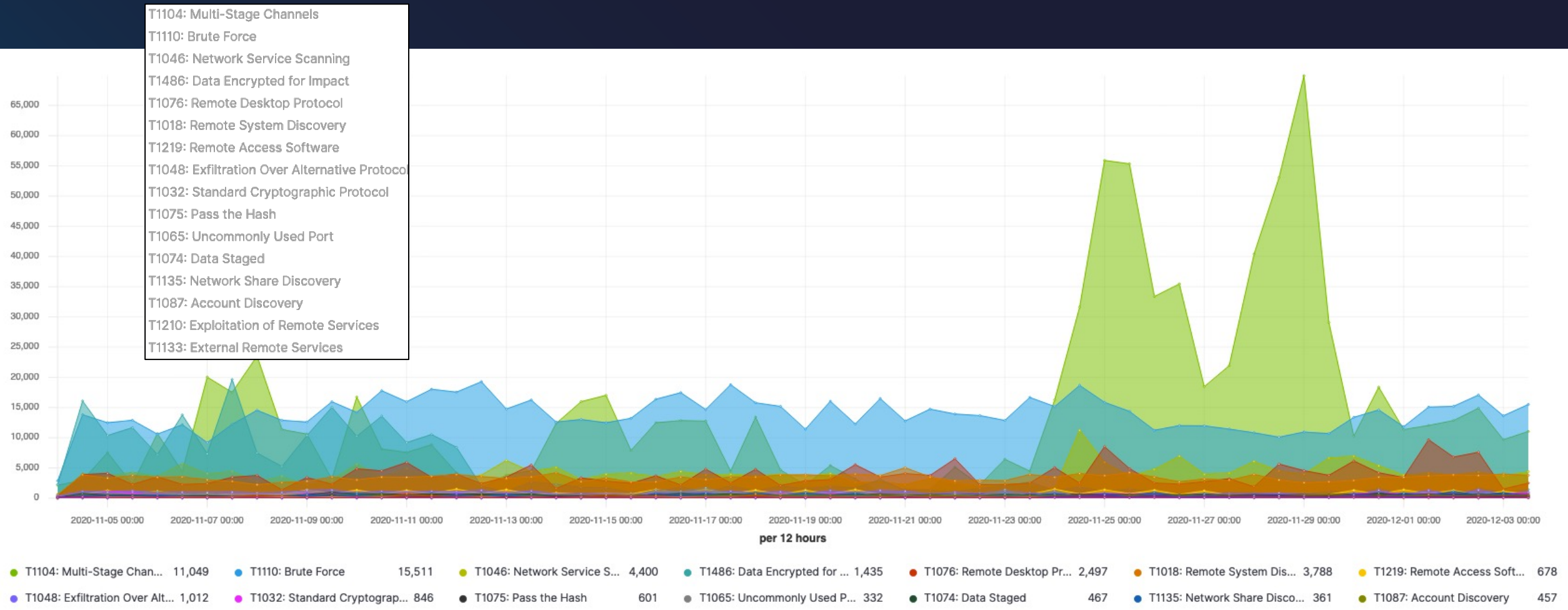
Analytics (Flows, IDS, DPI) done on each compute

No Network Changes, Taps and Packet Brokers

Complete network coverage

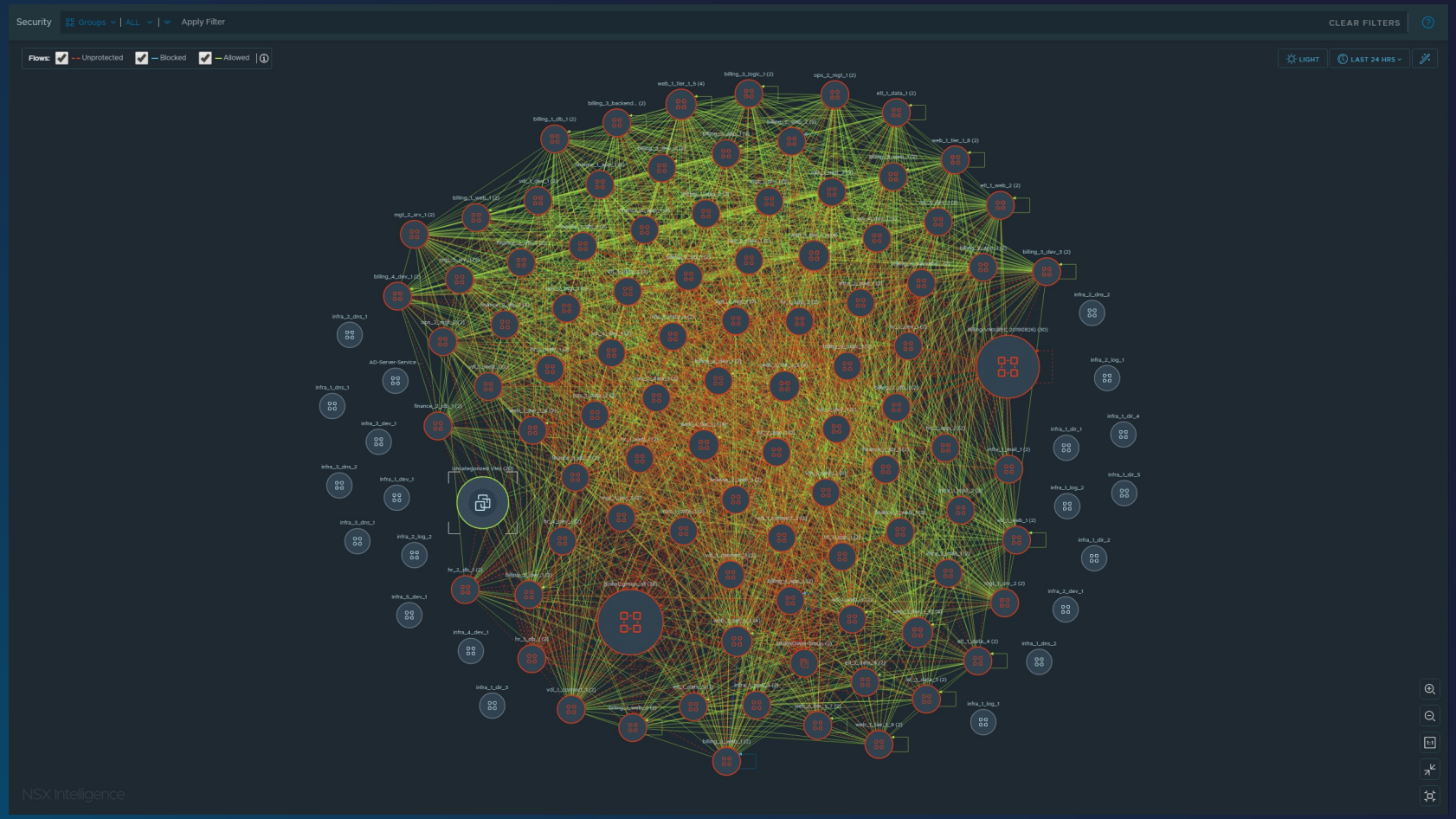
VMware Security Intelligence

Finding Security Relevance with Traditional Analytics solutions



VMware Security Intelligence

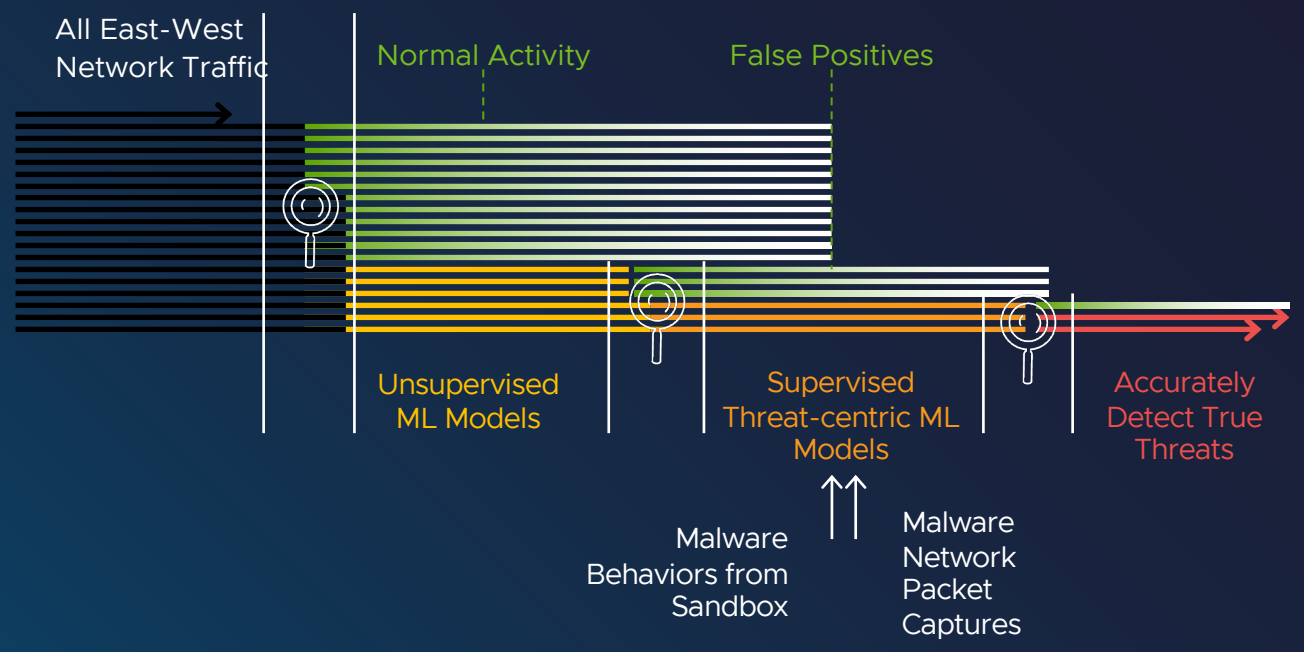
Scalable Contextual Visualization



- Security Intelligence provides Visualization of all NSX inventory and flows at <u>scale</u>
- Enables visibility of flow status in Group and VM communication maps.
- Highlighting a specific group will show related flows
- Rich filtering to drill down into more specific views

VMware Security Intelligence

Network Traffic Analysis



- **Detection of anomalous network behavior everywhere in the network**
- Machine-learning based detection of traffic anomalies with threat-centric models
- Applied to enriched flow and endpoint context collected by NSX intelligence
- 14 Detectors including, DNS Tunneling, Remote Services
- Every hypervisor is a sensor
- No need for TAPs, Monitoring Networks or network re-architecture

VMware Security Intelligence

Network Traffic Analysis: Domain Generation Algorithm

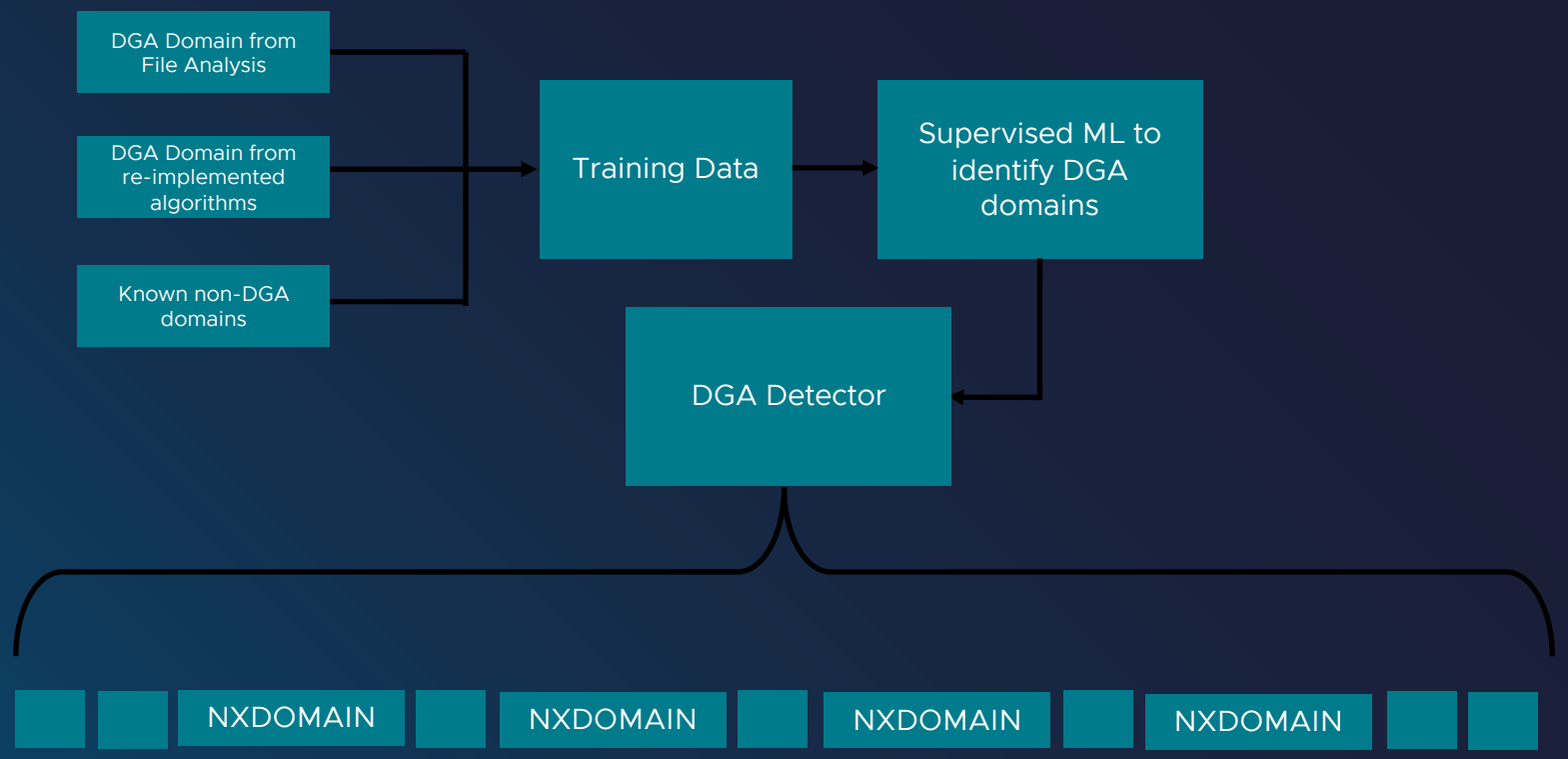
```python
class BazarBackdoor(AbstractDgaGenerator):
    """BazarBackdoor Domain Generation Algorithm."""

    VALID_CHARS = ["abcde", "cdef", "efgh", "ghi", "ijk", "klm"]

    def generate(self, date):
        """Generate BazarBackdoor domains given a date."""
        month = date.month
        year = date.year
        date_str = "{0:02d}{1:04d}".format(12 - month, year - 18)

        valid_chars = [list(_) for _ in BazarBackdoor.VALID_CHARS]
        for part1 in itertools.product(*valid_chars):
            domain = "".join(part1)
            for i, c in enumerate(part1):
                domain += chr(ord(c) + int(date_str[i]))
            domain += ".bazar"
            yield domain
```

- DGA is a hard-to-detect C2 technique
- Tries to connect to randomly generated domains, until it connects to a domain registered by the c2 servers
- Not readily detectable by signatures nor reputation-based solutions
- Yields an observable pattern of network traffic
- I.e. a series of failed DNS lookups to seemingly random domain, followed by a single successful connection to a random domain

Detect anomalies in the DNS lookups performed by an internal host that may be caused by DGA malware	Command and Control	To communicate with the dark side

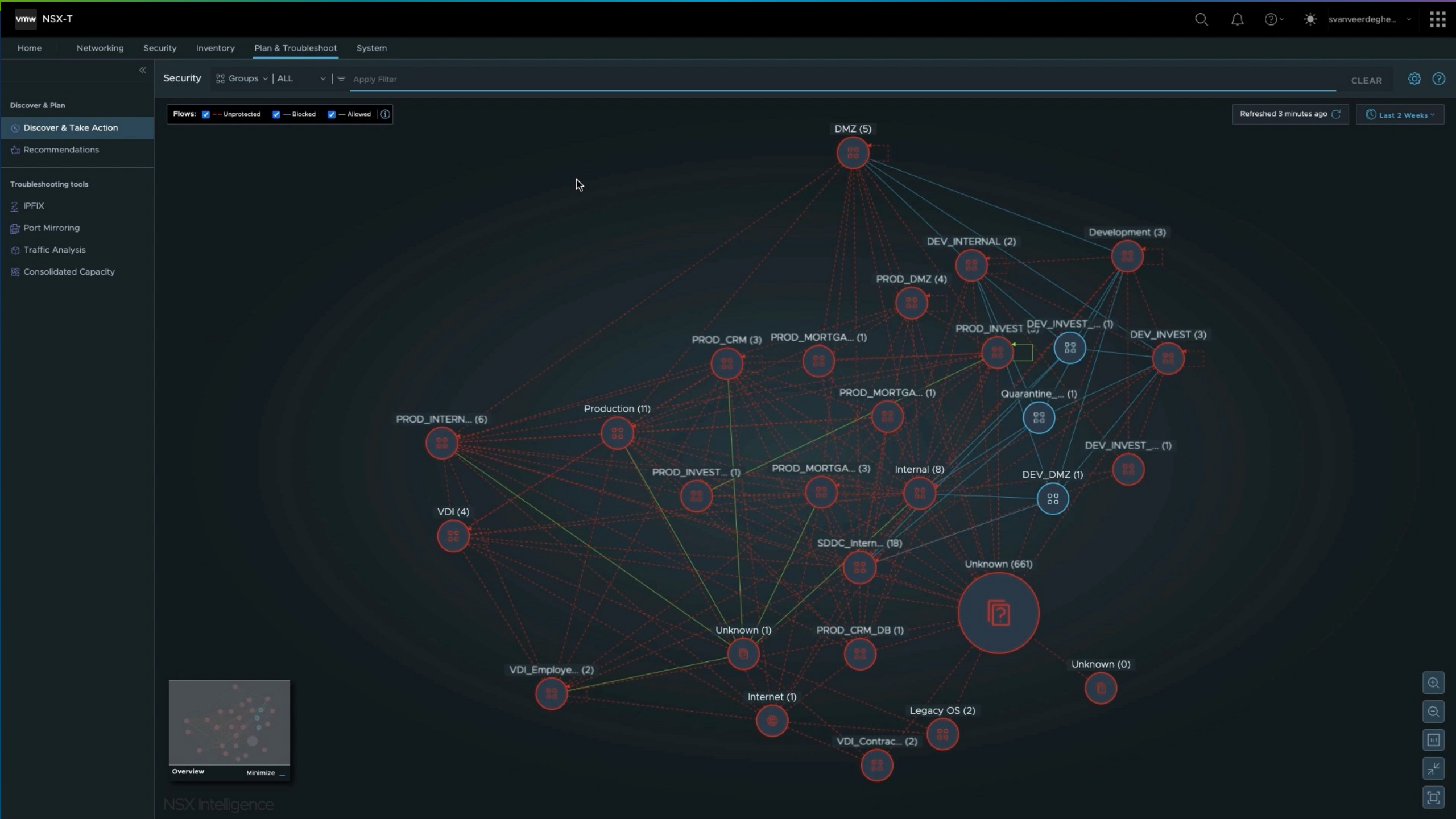
VMware Security Intelligence

Network Traffic Analysis: Domain Generation Algorithm



- DGA is a hard-to-detect C2 technique
- Tries to connect to randomly generated domains, until it connects to a domain registered by the c2 servers
- Not readily detectable by signatures nor reputation-based solutions
- Yields an observable pattern of network traffic
- I.e. a series of failed DNS lookups to seemingly random domain, followed by a single successful connection to a random domain

Detect anomalies in the DNS lookups performed by an internal host that may be caused by DGA malware	Command and Control	To communicate with the dark side


NSX-T
svanveerdeghe...
Home
Networking
Security
Inventory
Plan & Troubleshoot
System
Discover & Plan
Discover & Take Action
Recommendations
Troubleshooting tools
IPFIX
Port Mirroring
Traffic Analysis
Consolidated Capacity
Security
Groups
ALL
Apply Filter
CLEAR
Flows:
Unprotected
Blocked
Allowed
Refreshed 3 minutes ago
Last 2 Weeks
DMZ (5)
DEV_INTERNAL (2)
Development (3)
PROD_DMZ (4)
PROD_INVEST
DEV_INVEST_... (1)
DEV_INVEST (3)
PROD_CRM (3)
PROD_MORTGA... (1)
PROD_MORTGA... (1)
Quarantine_... (1)
Production (11)
PROD_INTERN... (6)
DEV_INVEST_... (1)
PROD_INVEST... (1)
PROD_MORTGA... (3)
Internal (8)
DEV_DMZ (1)
VDI (4)
SDDC_intern... (18)
Unknown (661)
Unknown (1)
PROD_CRM_DB (1)
Unknown (0)
VDI_Employe... (2)
Internet (1)
Legacy OS (2)
VDI_Contrac... (2)
Overview
Minimize
NSX Intelligence

Turning on the Lights

Comprehensive VMware Lateral Security Defense

Threat Analytics Powered by AI

VMware Lateral Security

Security Intelligence
Visibility | Micro-Segmentation Planning

App Discovery
Security Analytics
Rule Recommendations

Advanced Threat Prevention
IDS/IPS | NTA | NDR | Sandbox

Zero-day Exploits
Known Vulnerabilities
Anomaly Detection

Distributed Firewall

Gateway Firewall

Micro Segmentation
Segment Zones

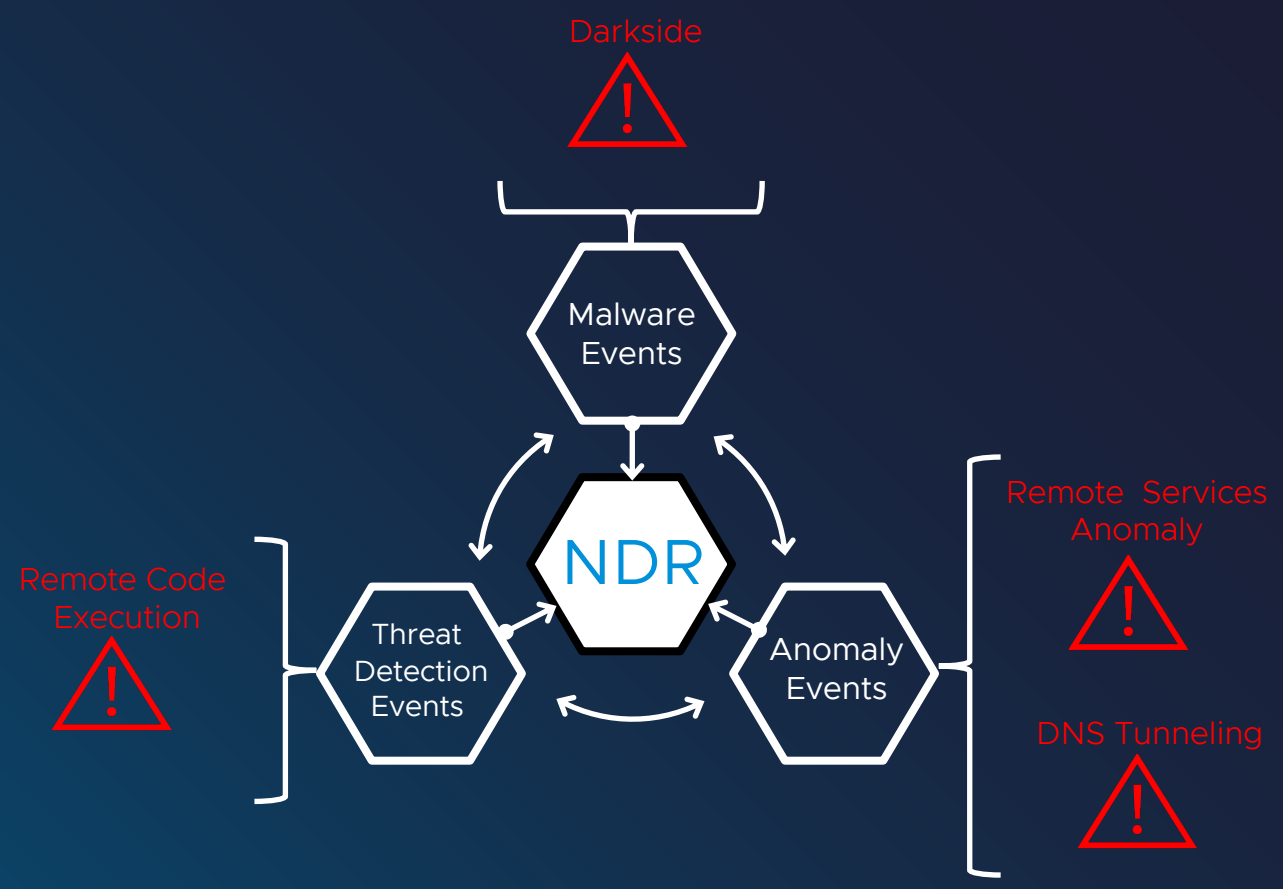
“Outdated security technology and processes and too many alerts or false negatives with detection software are listed among the top obstacles”

Scale Venture Partners 2020
Cybersecurity Perspectives

vmware by Broadcom

VMware Advanced Threat Prevention

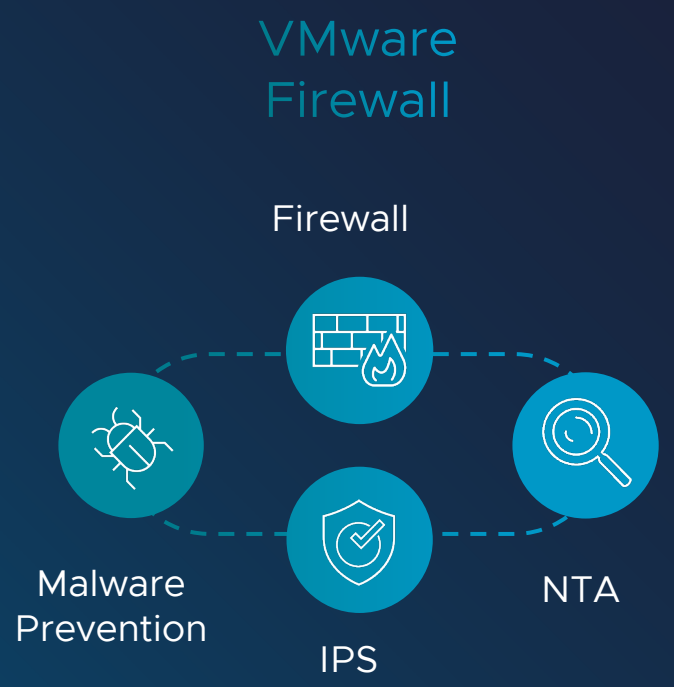
Network Detection and Response: Connecting the Attack Chain



- Scoring and Correlation of IDPS, Malware and Anomaly events into intrusion campaigns
- “Connect the attack chain” capability
- Provides security teams high fidelity by constantly correlating signals from distributed network sensors
- Correlation into threat campaigns rather than events allows SOC operators to focus on triaging only a small set of actionable threats.

VMware Advanced Threat Prevention

Network Detection and Response: Connecting the Attack Chain



ATT&CK TACTICS

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

91 **Campaign ID: 8b278b**
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Threats and hosts

- Malicious File... 3 Hosts
- DGA activity 2 Hosts
- Empire Agent 2 Hosts
- CryptoWall 1 Host
- Magnitude EK 1 Host
- Dnscat 1 Host

View threats details

192.168.20.151 | 192.168.100.181 | 192.168.20.211

View hosts details

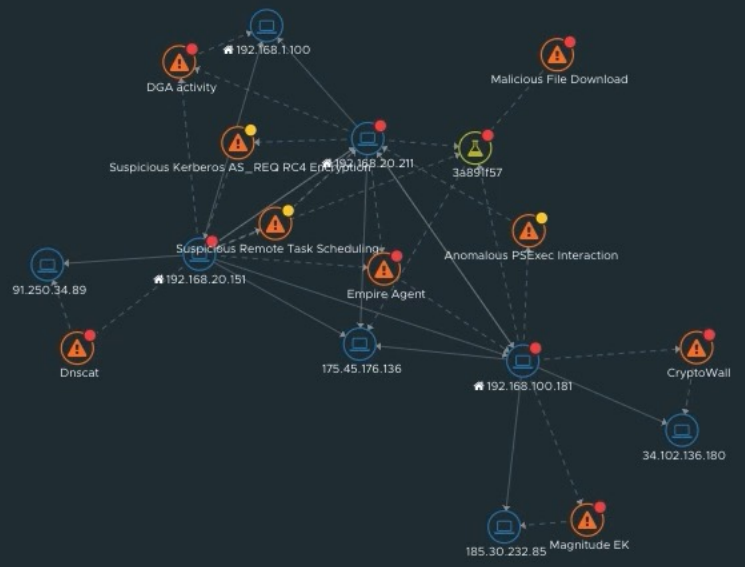
Impact: High Medium Low

Attack stages

- delivery 3 Hosts
- exploitation 1 Host
- command and control 3 Hosts
- credential access 1 Host
- discovery
- lateral movement 3 Hosts
- collection
- exfiltration 1 Host

Activity No Activity

Campaign blueprint



Today's Security Realities

Paradigm Shift in Ransomware Attacks

Maze Ransomware

Sophisticated Ransomware

Maze ransomware, previously known as "ChaCha", was discovered in May 2019. In addition to encrypting files on victim machines for impact, Maze operators conduct information stealing campaigns prior to encryption and post the information online to extort affected companies.

FIN6 is a cybercrime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.

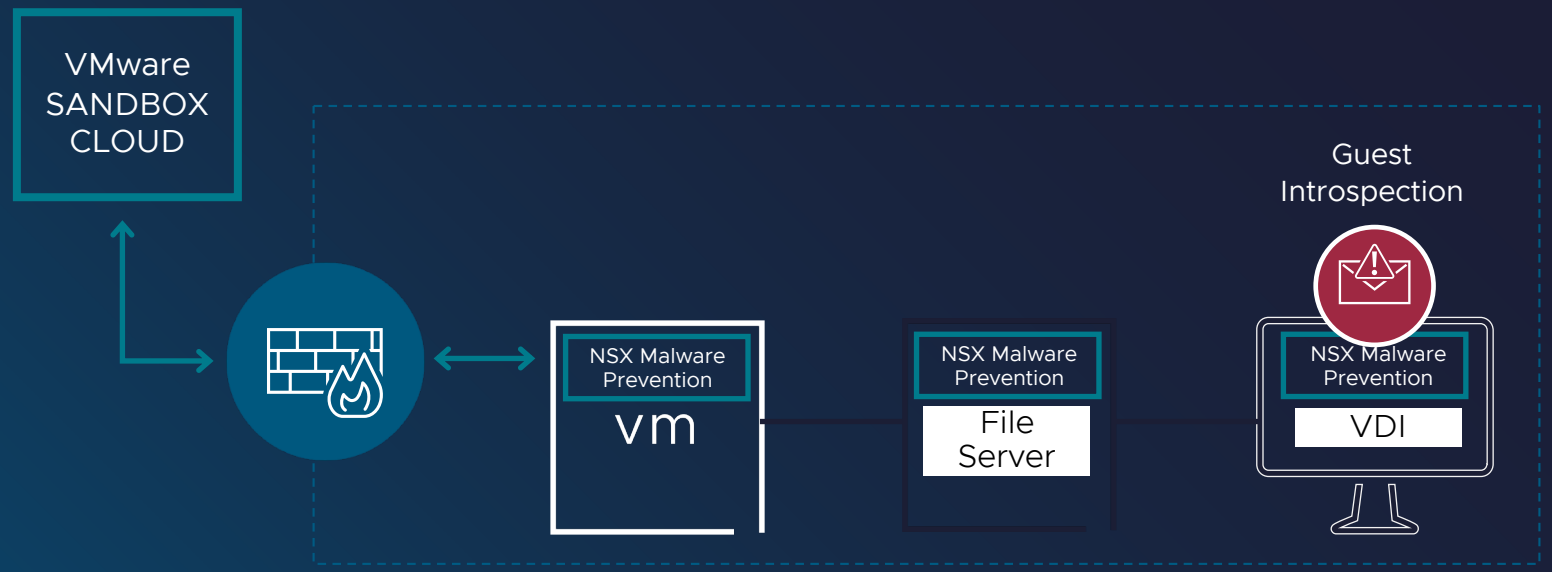
https://attack.mitre.org/groups/G0037/
Associated Groups: Magecart Group 6, ITG08, Skeleton Spider

- mitre-attack-pattern :: Scheduled Task - T1053.005
- mitre-enterprise-attack-attack-pattern :: Windows Management Instrumentation - T1047
- mitre-attack-pattern :: Service Stop - T1489
- mitre-enterprise-attack-attack-pattern :: System Information Discovery - T1082
- mitre-attack-pattern :: Msiexec - T1218.007
- mitre-enterprise-attack-attack-pattern :: Execution through API - T1106
- mitre-attack-pattern :: Binary Padding - T1027.001
- mitre-enterprise-attack-attack-pattern :: Indicator Removal on Host - T1070
- mitre-attack-pattern :: Dynamic Resolution - T1568
- mitre-attack-pattern :: Masquerade Task or Service - T1036.004
- mitre-enterprise-attack-attack-pattern :: System Network Connections Discovery - T1049
- mitre-enterprise-attack-attack-pattern :: Process Discovery - T1057
- mitre-attack-pattern :: Registry Run Keys / Startup Folder - T1547.001
- mitre-attack-pattern :: Disable or Modify Tools - T1562.001
- mitre-enterprise-attack-attack-pattern :: Obfuscated Files or Information - T1027
- mitre-attack-pattern :: Run Virtual Instance - T1564.006
- mitre-attack-pattern :: Data Encrypted for Impact - T1486
- mitre-attack-pattern :: System Language Discovery - T1614.001
- mitre-attack-pattern :: Windows Command Shell - T1059.003
- mitre-attack-pattern :: Web Protocols - T1071.001
- mitre-attack-pattern :: Dynamic-link Library Injection - T1055.001
- mitre-attack-pattern :: Inhibit System Recovery - T1490
- mitre-attack-pattern :: System Shutdown/Reboot - T1529
- mitre-enterprise-attack-intrusion-set :: FIN6 - G0037

1. Conti Ransomware had a playbook to disable all major security software

VMware Advanced Threat Prevention

Malware Prevention



- Detection & Prevention of known and unknown malicious files
- Windows and Linux Support
- Hash lookup, Local (static) analysis and cloud-based dynamic analysis
- Guest-introspection based file-extraction and blocking for DFW
- No hairpinning, network-latency or re-architecture

VMware Advanced Threat Prevention

Malware Prevention: Local and Cloud Analysis

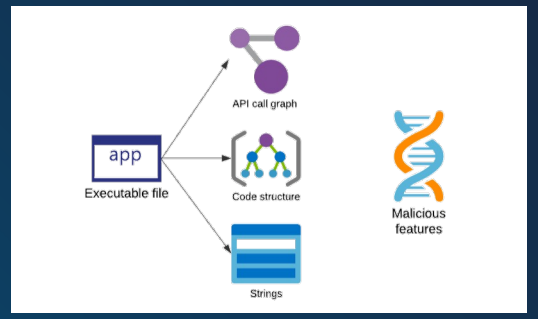
Local Analysis

Prefiltering of clearly Benign Files

Prefiltering of obvious Malicious Files

- File signature, file structure, URLs, JS scripts, VBA macros, XL4 code, key strings Structure analysis, YARA rules, Images analysis (OCR), etc

Determines if Cloud Analysis is needed



Cloud Analysis

Files are sent to the NSX Advanced Threat Prevention Service (Lastline New Next-Gen Sandbox Cloud)

Behavior Analysis

High-Visibility– Full visibility into malware actions (disk, memory, network, cpu instruction)

Hard to fingerprint – outside the guest OS instrumentation

Faster File Analysis – than previous Sandbox generation

Resistant to evasion – dynamically responds to evasion tricks (such as dormant code in memory)

91 **Campaign ID: 8b278b**
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Overview | Hosts | Timeline | History | Evidence

Threats and hosts

- Malicious File... 3 Hosts
- DGA activity 2 Hosts
- Empire Agent 2 Hosts
- CryptoWall 1 Host
- Magnitude EK 1 Host
- Dnscat 1 Host

View threats details

192.168.20.151 | 192.168.100.181 | 192.168.20.211

View hosts details

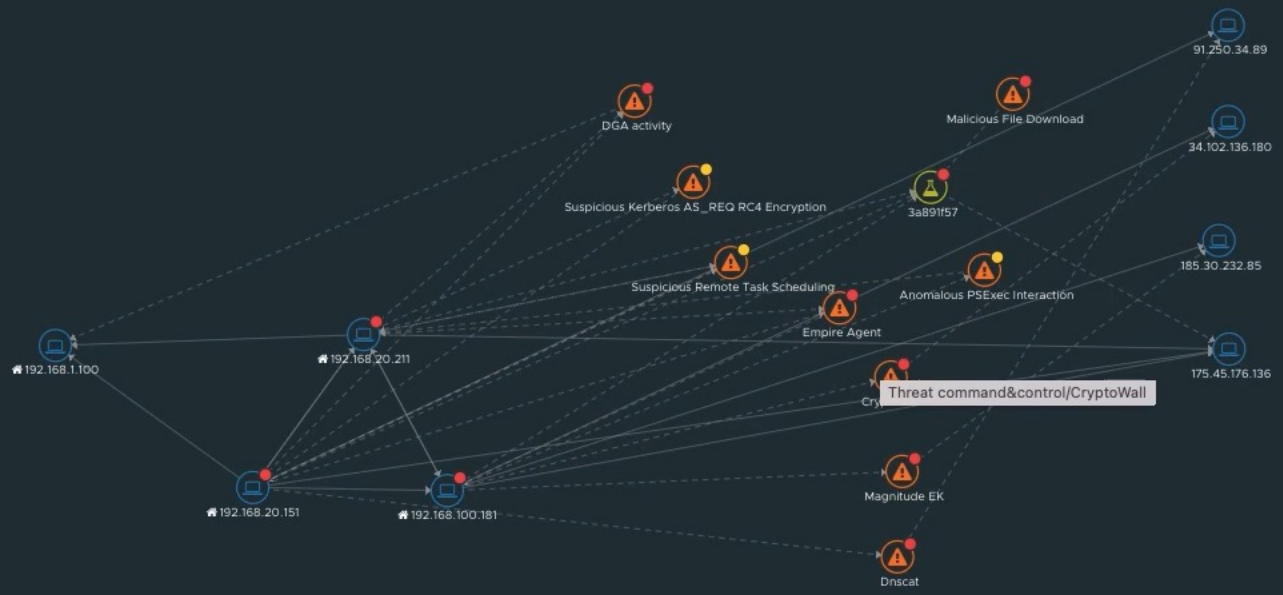
Impact: High Medium Low

Attack stages

- delivery 3 Hosts
- exploitation 1 Host
- command and control 3 Hosts
- credential access 1 Host
- discovery
- lateral movement 3 Hosts
- collection
- exfiltration 1 Host

Activity | No Activity

Campaign blueprint



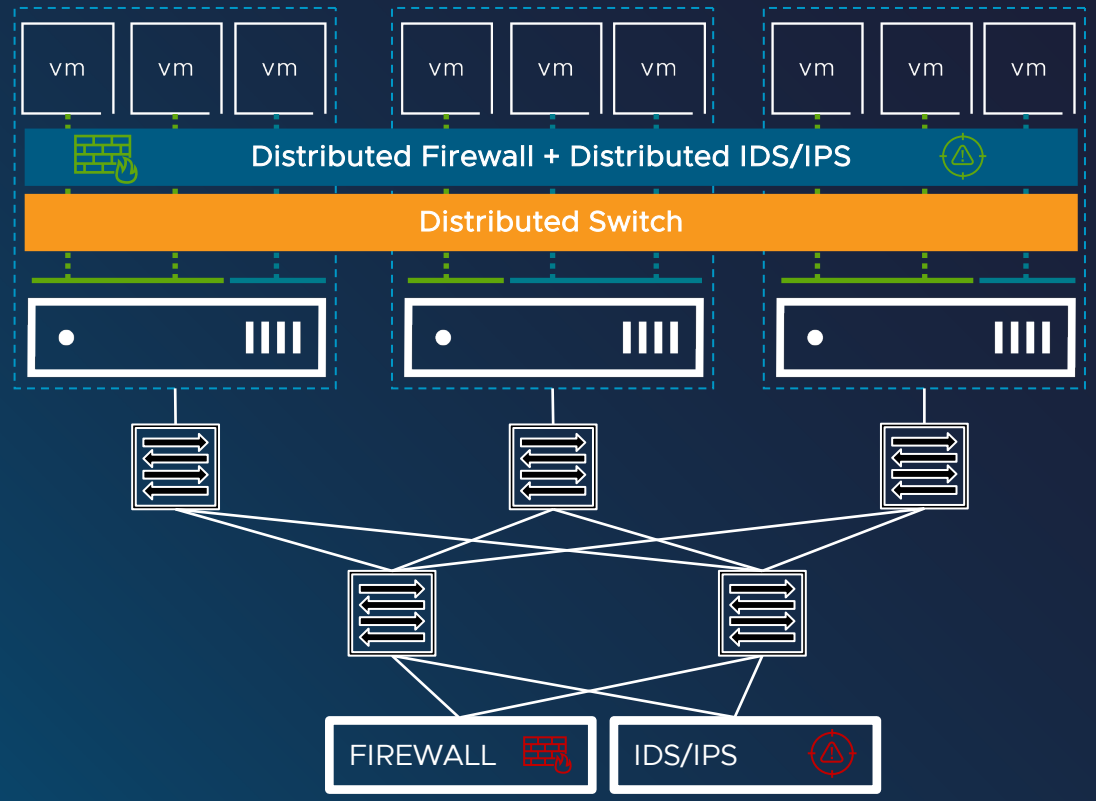
“60% of breach victims said they were breached due to an unpatched known vulnerability where the patch was not applied”

Ponemon Institute

vmware by Broadcom

VMware Advanced Threat Prevention

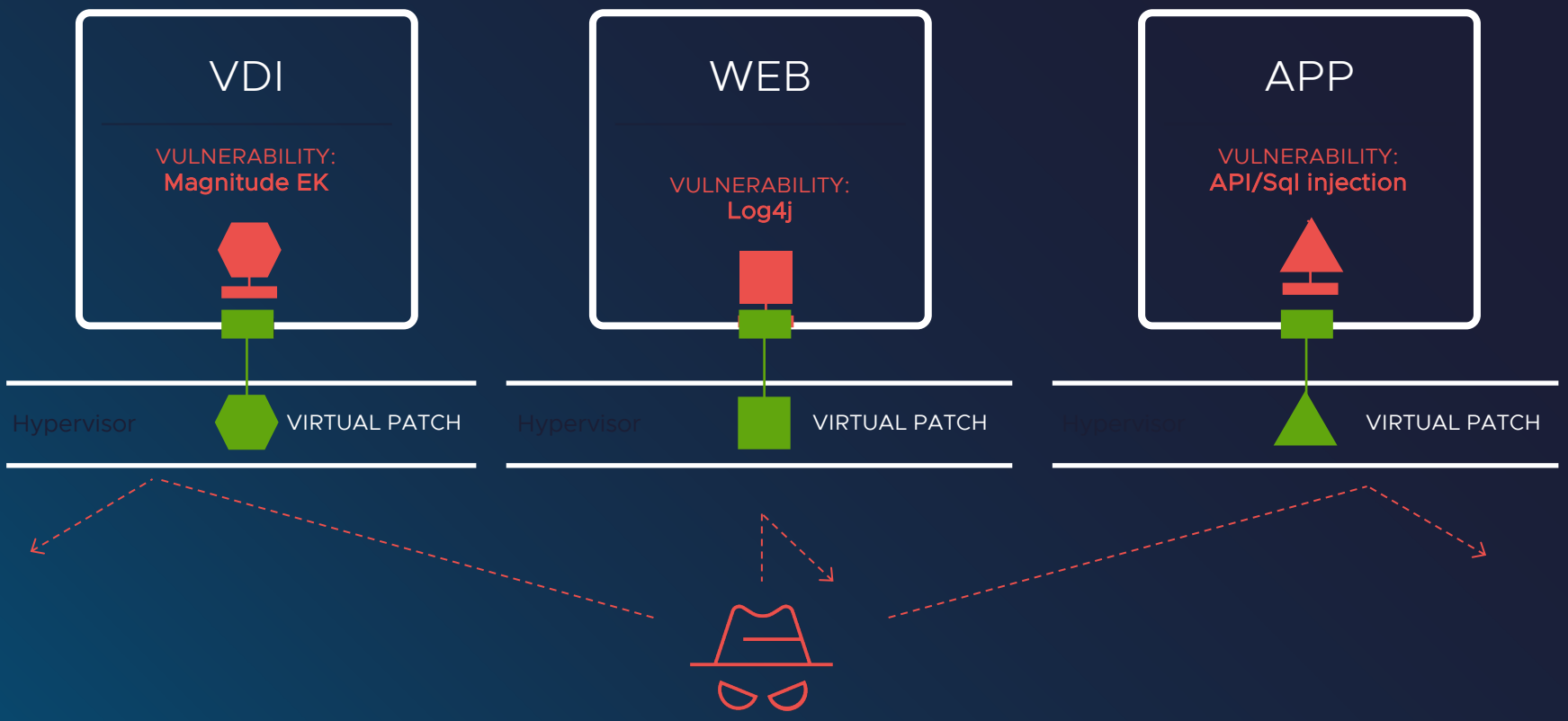
Intrusion Detection and Prevention: Preventing Exploits at every workload



- Distributed & Built-in Analysis – scales linearly with workloads, no blind-spots
- Curated Signature Distribution – fewer false positives, lower computational overhead on host
- Context-based Threat Detection and scoring – reduced need for signature tuning, better alert prioritization
- Policy & State Mobility - simplify operations, eliminate stale / redundant policies

VMware Advanced Threat Prevention

Intrusion Detection and Prevention: Virtual Patching with the Distributed IDPS



Patching Dilemma

Patching everything is difficult and resource intensive

Patching cycles are lengthy and often require maintenance window/downtime

Patches may not be available for older systems

Virtual Patching

Compensating control by front-ending vulnerable workloads with a dedicated IDPS signature set

Protection regardless of where the attack comes from

Provides protection from network exploits until actual software patch is applied

VMware Advanced Threat Prevention

Intrusion Detection and Prevention: Signatures

	VMware Distributed and Gateway IDPS
Signature Sources	Trustwave Spiderlab SLR, Emerging Threat ET, NSX
Signature Curation	VMware TAU
Signature Update Check Frequency	20 Minutes
Typical Signature Set Release Cadence	~ Every day
Detection Mechanism	Signatures, LUA Scripts
Signature Severities	Critical, High, Medium, Low, Suspicious
Default VMware Action	Alert Drop Reject (majority)
Event Details	Attacker/Target, Severity, Product/Users/VMs affected, CVSS/CVE, Attack Target, Attack Type, Detailed Attack History, Bytes, Action taken, Impact Score, Mitre Tactic & Technique (only in UI)
Event Scoring	Confidence, Risk, Impact/Severity, CVSS
Event Promotion	Promotion of information al events to threat events based on context (NDR)

VMware Advanced Threat Prevention

ATP/NDR Portfolio

VMware ATP

Available for VMware Firewall

No dedicated sensors required: distributed firewall and gateway firewall are ‘sensors’

IDS/IPS, NTA, sandboxing included

Aligned with MITRE ATT&CK framework

VMware ATP Standalone

Standalone product deployed on-prem

Sensors deployed to tap traffic; additional components (Engine, Mgr, Data Nodes) reqd. for data processing

IDS, NTA, sandboxing included

Aligned with MITRE ATT&CK framework

91 Campaign ID: 8b278b
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Overview | Hosts | Timeline | History | Evidence

Sort by: Earliest (by start time) | Search threats | Show closed threats

Apr 25, 21:14:46 - Apr 25, 21:14:46

192.168.100.181 | 100 MALICIOUS FILE DOWNLOAD | EVIDENCE SUMMARY: 1 type: File download | Latest stage: Delivery | OPEN | NEXT STEPS

Evidence
21:14:46 Apr 25 | File download /msteemsupdater.zip | Confidence: 80

Network interactions & network IOCs
175.45.176.136

Supporting data
1 detection events
View all threat details

Apr 25, 21:14:47 - Apr 25, 21:14:47

192.168.100.181 | 65 MAGNITUDE EK | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Exploitation | OPEN | NEXT STEPS

Apr 25, 21:18:12 - Apr 25, 21:21:35

192.168.100.181 | 70 CRYPTOWALL | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.100.181 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.20.211 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Apr 25, 21:47:50 - Apr 25, 21:53:15

192.168.20.211 | 80 DGA ACTIVITY | EVIDENCE SUMMARY: 1 type: Anomaly | Latest stage: Command and Control | OPEN | NEXT STEPS

Apr 25, 21:48:14 - Apr 25, 21:48:14

192.168.20.211 | 75 EMPIRE AGENT | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

EVIDENCE

File download

REFERENCE EVENT

This alert was raised because host 192.168.100.181 has downloaded a malicious file from 175.45.176.136.

FILE TYPE: ZipArchiveFi
CONFIDENCE: 80
SHA1: 210844e8b0ff0fd2f79e8162e06ced82209dd4ee

Malware Identification
Analyst report

ANTIVIRUS CLASS: RANSOMWARE, TROJAN
ANTIVIRUS FAMILY: BULZ, CRYPTODEF

MALWARE: CRYPTOWALL | SUSPICIOUS GEOLOCATION QUERY

BEHAVIOR OVERVIEW (19)

- 100 Family — Ransomware specific behavior
- 100 Network — Using domain from low-reputation servers (command&control)
- 80 Disable — Stopping the Windows Security Center service

Expand for more

Open in...
Google | Shodan | Threatminer | UrlHaus

Expand for more

Download details
Analyst report

FILE NAME: /msteemsupdater.zip
URL: http://175.45.176.136/msteemsupdater.zip,

91 Campaign ID: 8b278b
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Overview | Hosts | Timeline | History | Evidence

Sort by: Earliest (by start time) | Search threats | Show closed threats

Apr 25, 21:14:46 - Apr 25, 21:14:46

192.168.100.181 | 100 MALICIOUS FILE DOWNLOAD | EVIDENCE SUMMARY: 1 type: File download | Latest stage: Delivery | OPEN | NEXT STEPS

Evidence
21:14:46 Apr 25 — File download /msteemsupdater.zip — Confidence: 80

Network interactions & network IOCs
175.45.176.136

Supporting data
1 detection events
View all threat details

Apr 25, 21:14:47 - Apr 25, 21:14:47

192.168.100.181 | 65 MAGNITUDE EK | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Exploitation | OPEN | NEXT STEPS

Evidence
21:14:47 Apr 25 — Signature llrules:14696191012... — Confidence: 90

Network interactions & network IOCs
185.30.232.85

Supporting data
1 detection events
View all threat details

Apr 25, 21:18:12 - Apr 25, 21:21:35

192.168.100.181 | 70 CRYPTOWALL | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

Evidence
et:2018452
21:18:12 Apr 25 — Signature et:2018452 — Confidence: 70

Network interactions & network IOCs
34.102.136.180
172.67.144.44

Supporting data
2 detection events
View all threat details

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.100.181 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.20.211 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

EVIDENCE SUMMARY

Signature

REF EVENT

This alert was raised because traffic from host 192.168.100.181 to 34.102.136.180 has matched network signatures for threat command&control.

Threat
CryptoWall

Threat Class
command&control

Activity
N/A

Confidence
70

First Seen: Apr 25, 21:18:12
Last Seen: Apr 25, 21:21:35
Duration: 3 minutes

Reference Event Traffic
192.168.100.181
34.102.136.180

Detector Summary — More details

Detector Name
et:2018452

Goal
<!-- auto-generated -->Detect CryptoWall Check-in.

IDS Rule
View rule (if available)

91 Campaign ID: 8b278b
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Apr 25, 21:18:12 - Apr 25, 21:21:35

192.168.100.181 | 70 CRYPTOWALL | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.100.181 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Evidence
21:24:56 Apr 25 | **Unusual behavior** lateral movement | Confidence: 90

Network interactions & network IOCs
192.168.20.211

Supporting data
1 detection events
View all threat details

Apr 25, 21:24:56 - Apr 25, 21:42:29

192.168.20.211 | 25 ANOMALOUS PSEXEC INTERACTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Evidence
21:24:56 Apr 25 | **Unusual behavior** lateral movement | Confidence: 70

Network interactions & network IOCs
192.168.100.181

Supporting data
1 detection events
View all threat details

Apr 25, 21:47:50 - Apr 25, 21:53:15

192.168.20.211 | 80 DGA ACTIVITY | EVIDENCE SUMMARY: 1 type: Anomaly | Latest stage: Command and Control | OPEN | NEXT STEPS

Apr 25, 21:48:14 - Apr 25, 21:48:14

192.168.20.211 | 75 EMPIRE AGENT | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

Apr 25, 21:50:12 - Apr 25, 21:50:12

192.168.20.211 | 100 MALICIOUS FILE DOWNLOAD | EVIDENCE SUMMARY: 1 type: File download | Latest stage: Delivery | OPEN | NEXT STEPS

Apr 25, 21:53:41 - Apr 25, 22:02:34

192.168.20.211 | 20 SUSPICIOUS REMOTE TASK SCHEDULING | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

HOST SUMMARY

100 192.168.20.211

VIEW PROFILE

1 CAMPAIGN
1 THREAT

Details
HOST NAME
No host names found
ASSOCIATED VM(S) - VIEW VM INVENTORY
PROD-CRM-APP-1
Apr 25, 21:00:00 - 21:59:59 — (60 minutes)

Active campaigns 1
91 Campaign ID: 2f24...b278b 3 hosts total

Threats 1 View threats
25 Anomalous PSExec Interaction
Anomalous Network Interaction
Apr 25, 21:24:56 - 21:42:29 — (18 minutes)

91 Campaign ID: 8b278b
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

Apr 25 | Confidence: 70

View all threat details

Apr 25, 21:47:50 - Apr 25, 21:53:15

192.168.20.211 | 80 DGA ACTIVITY | EVIDENCE SUMMARY: 1 type: Anomaly | Latest stage: Command and Control | OPEN | NEXT STEPS

Evidence
21:47:50 Apr 25 | Anomaly dga | Confidence: 80

Network interactions & network IOCs
192.168.1.100

Supporting data
1 detection events
View all threat details

Apr 25, 21:48:14 - Apr 25, 21:48:14

192.168.20.211 | 75 EMPIRE AGENT | EVIDENCE SUMMARY: 1 type: Signature | Latest stage: Command and Control | OPEN | NEXT STEPS

Evidence
21:48:14 Apr 25 | Signature et:2027512 | Confidence: 75

Network interactions & network IOCs
192.168.100.181

Supporting data
1 detection events
View all threat details

Apr 25, 21:50:12 - Apr 25, 21:50:12

192.168.20.211 | 100 MALICIOUS FILE DOWNLOAD | EVIDENCE SUMMARY: 1 type: File download | Latest stage: Delivery | OPEN | NEXT STEPS

Evidence
21:50:12 Apr 25 | File download /msteemsupdater.zip | Confidence: 80

Network interactions & network IOCs
175.45.176.136

Supporting data
1 detection events
View all threat details

Apr 25, 21:53:41 - Apr 25, 22:02:34

192.168.20.211 | 20 SUSPICIOUS REMOTE TASK SCHEDULING | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Lateral Movement | OPEN | NEXT STEPS

Apr 25, 21:53:44 - Apr 25, 21:53:44

192.168.20.211 | 20 SUSPICIOUS KERBEROS AS_REQ RC4 ENCRYPTION | EVIDENCE SUMMARY: 1 type: Unusual behavior | Latest stage: Credential Access | OPEN | NEXT STEPS

Apr 25, 21:57:58 - Apr 25, 22:06:51

EVIDENCE SUMMARY

Signature

REF EVENT

This alert was raised because traffic from host 192.168.20.211 to 192.168.100.181 has matched network signatures for threat command&control.

Threat
Empire Agent

Threat Class
command&control

Activity
command&control

Confidence
75

First Seen: Apr 25, 21:48:14
Last Seen: Apr 25, 21:48:14
Duration: < 1 second

Reference Event Traffic

192.168.20.211
192.168.100.181

Detector Summary

More details

Detector Name
et:2027512

Goal
<!-- auto-generated -->Detect Possible PowerShell Empire Activity Outbound.

IDS Rule
View rule (if available)

91 Campaign ID: 8b278b
2022-04-25 – 2022-04-25

Latest stage: Exfiltration | Affected hosts: 3 | Threats: 9 | State: Open

192.168.20.151 — 20 SUSPICIOUS REMOTE TASK SCHEDULING
EVIDENCE SUMMARY: 1 type: Unusual behavior
Latest stage: Lateral Movement
OPEN | NEXT STEPS

Evidence
21:57:58 Apr 25 — **Unusual behavior** lateral movement
Confidence: 50

Network interactions & network IOCs
192.168.20.211

Supporting data
1 detection events
View all threat details

Apr 25, 22:13:45 - Apr 25, 22:19:00

192.168.20.151 — 80 DGA ACTIVITY
EVIDENCE SUMMARY: 1 type: Anomaly
Latest stage: Command and Control
OPEN | NEXT STEPS

Evidence
22:13:45 Apr 25 — Anomaly dga
Confidence: 80

Network interactions & network IOCs
192.168.1.100

Supporting data
1 detection events
View all threat details

Apr 25, 22:13:58 - Apr 25, 22:13:58

192.168.20.151 — 75 EMPIRE AGENT
EVIDENCE SUMMARY: 1 type: Signature
Latest stage: Command and Control
OPEN | NEXT STEPS

Evidence
22:13:58 Apr 25 — Signature et:2027512
Confidence: 75

Network interactions & network IOCs
192.168.100.181

Supporting data
1 detection events
View all threat details

Apr 25, 22:15:56 - Apr 25, 22:15:56

192.168.20.151 — 100 MALICIOUS FILE DOWNLOAD
EVIDENCE SUMMARY: 1 type: File download
Latest stage: Delivery
OPEN | NEXT STEPS

Evidence
22:15:56 Apr 25 — File download /msteemsupdater.zip
Confidence: 80

Network interactions & network IOCs
175.45.176.136

Supporting data
1 detection events
View all threat details

Apr 25, 22:19:20 - Apr 25, 22:19:21

192.168.20.151 — 65 DNSCAT
EVIDENCE SUMMARY: 1 type: Signature
Latest stage: Exfiltration
OPEN | NEXT STEPS

HOST SUMMARY
100 192.168.20.151
VIEW PROFILE

1 CAMPAIGN
1 THREAT

Details
HOST NAME
No host names found
ASSOCIATED VM(S) - VIEW VM INVENTORY
PROD-MORTGAGE-APP-1
Apr 25, 22:00:00 - 22:59:59 — (60 minutes)
PROD-CRM-APP-1
Apr 25, 21:00:00 - 22:59:59 — (2 hours)

Active campaigns 1
91 Campaign ID: 2f24...b278b — 3 hosts total

Threats 1 — View threats
20 Suspicious Remote Task Scheduling
Anomalous Network Interaction
Apr 25, 21:57:58 - 22:06:51 — (9 minutes)

Security Overview

Threat Detection & Response | Configuration | Capacity

Campaigns | IDS/IPS | FQDN Analysis | URL Filtering | Malware Prevention | Suspicious Network Activity | TLS Inspection

REFRESH

Last 1 Week

Active Campaigns
0

In Progress High Impact Campaigns
0

Open High Impact Campaigns
0

All VMs Affected
0

GO TO CAMPAIGNS

Turning on the Lights

Comprehensive VMware Lateral Security Defense

Threat Analytics Powered by AI

VMware Lateral Security

Security Intelligence
Visibility | Micro-Segmentation Planning

App Discovery
Security Analytics
Rule Recommendations

Advanced Threat Prevention
IDS/IPS | NTA | NDR | Sandbox

Zero-day Exploits
Known Vulnerabilities
Anomaly Detection

Distributed Firewall

Gateway Firewall

Micro Segmentation
Segment Zones

Today's Security Realities

Lack of Internal Segmentation leads to Unmitigated lateral movement

44%

of breaches perform some form of lateral movement[1]

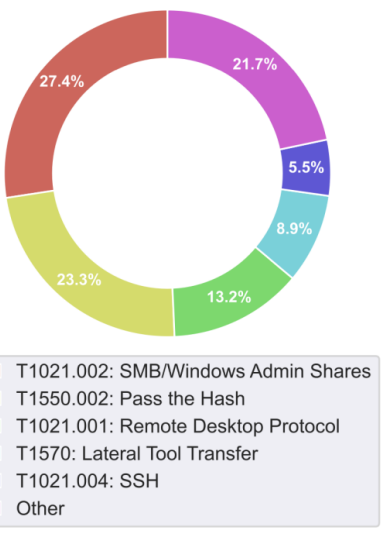
2-3 Hops

and very rarely 4, making for swift closing and laser focused propagation attempts[2]

64%

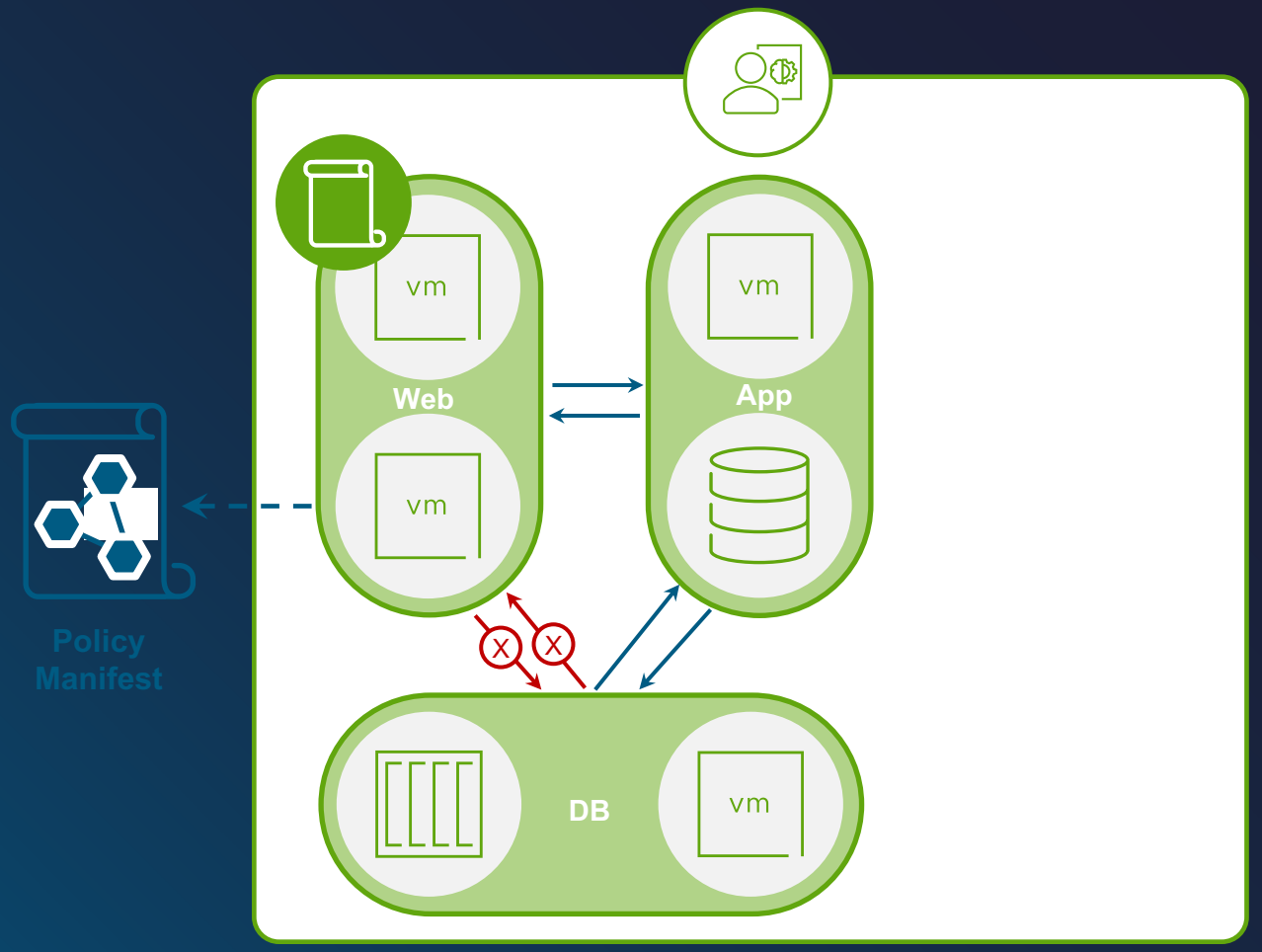
use of the Samba service, Pass the Hash and the Remote Desktop Protocol

"The Remote Desktop Protocol and SSH connections are probably two of the easiest techniques to perform lateral movement. These intrusion events are particularly difficult to identify as they easily get lost among the events associated with legitimate administrative activity. "



VMware Firewall

Distributed Firewall: Prevent Lateral Movement without network changes



- **Network-Independent L2-L7 Transparent Firewall**
- VM, BM and K8S
- Zones and Infrastructure Segmentation
- Application Isolation and Micro-segmentation
- VLAN and Overlay-backed
- Applied directly to VDS DVPG
- L7 APP-ID
- FQDN/Outbound Filtering
- User-based Firewalling

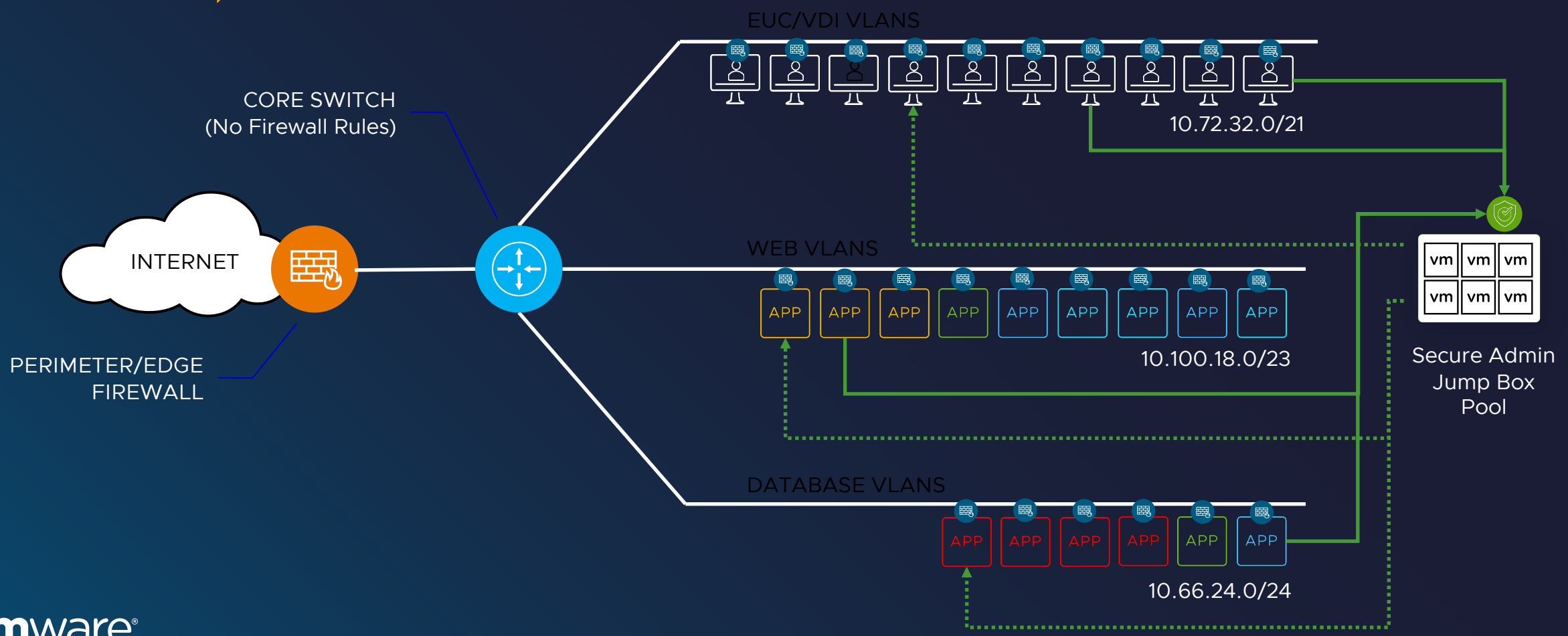
VMware Firewall

Block unsecure protocols everywhere

2 FIREWALL RULES

1. Src: [Jump] to Dst: [Any] [RDP_SSH] Action: Allow
2. Src: [Any] to Dst: [Any] [RDP_SSH] Action: Drop

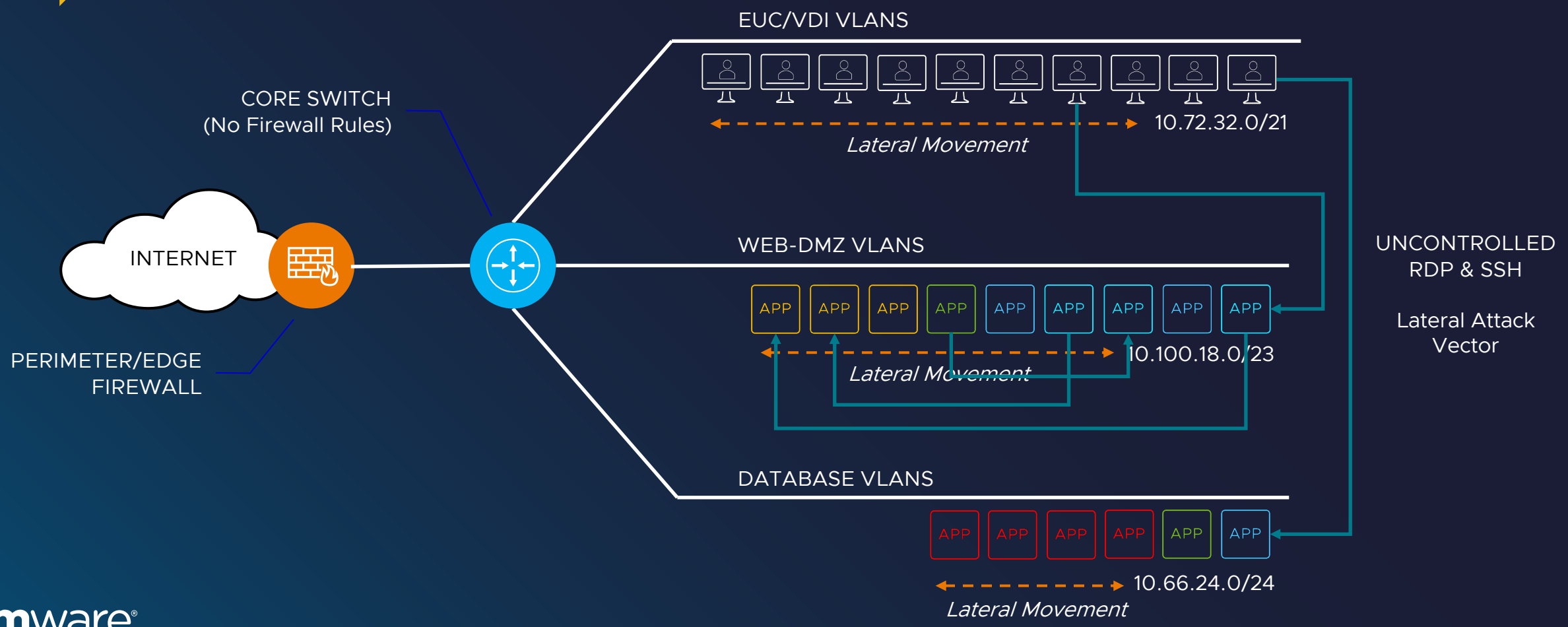
BEFORE *AFTER*



VMware Firewall

RDP/SSH Attack Vector - The problem

BEFORE *AFTER*



VMware Firewall

RDP/SSH Attack Vector - The solution

BEFORE *AFTER*

2 FIREWALL RULES

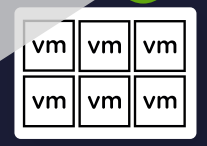
1. Src: [Jump_Pool] to Dst: [Any] [RDP_SSH] Action: Allow
2. Src: [Any] to Dst: [Any] [RDP_SSH] Action: Drop

IPS SIGNATURE PROFILE: Secure Jump Box

1094259 - NSX - Detect usage of DNS-over-HTTPS to OpenDNS/doh.opendns.com
1094261 - NSX - Detect usage of DNS-over-HTTPS to Quad9/149.112.112.xxx
1098482 - NSX - (Command and Control) Detect connection attempts to pastebin.com
2012170 - ET GAMES Blizzard Web Downloader Install Detected
4103300 - SLR Alert - Splashtop Remote Management API Access Detected
2020371 - ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 45
2024297 - ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010
4103270 - SLR Alert - AnyDesk User-Agent Detected (Associated w/ Malware Groups)
2026078 - ET INFO Inbound PowerShell Checking for Virtual Host (Win32_BaseBoard WMI)

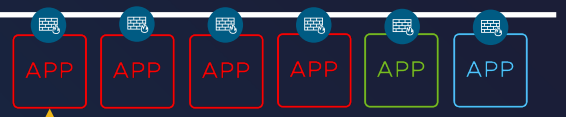
CORE SWITC
(No Firewall Rules

PERIMETER/EDGE
FIREWALL



Secure Admin
Jump Box
Pool

DATABASE VLANS

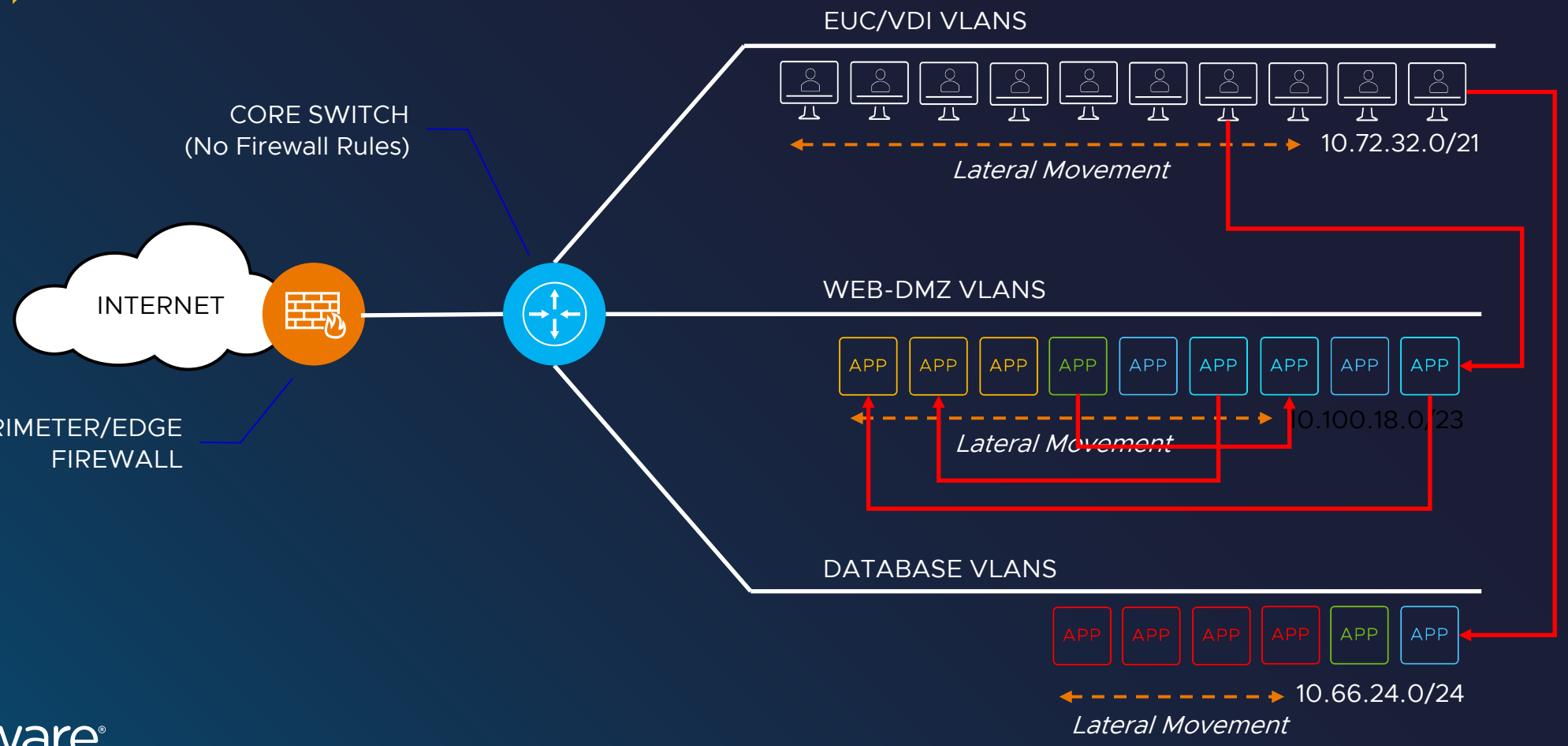


10.66.24.0/24

VMware Firewall

Known Unsecure Protocols - The problem

BEFORE AFTER



UNSECURE
Telnet, FTP, SMBv1, TLSv1.0

Lateral Attack Vector

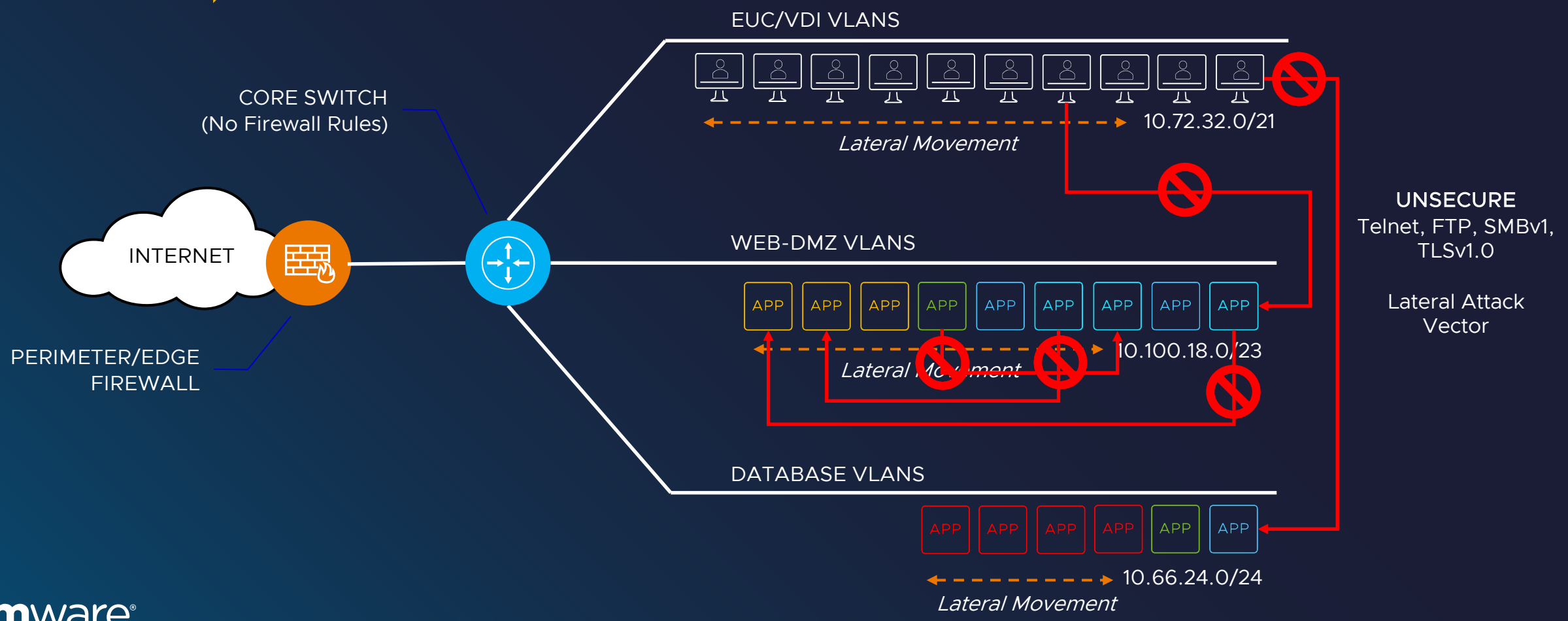
VMware Firewall

Known Unsecure Protocols - The solution

1 SIMPLE RULE

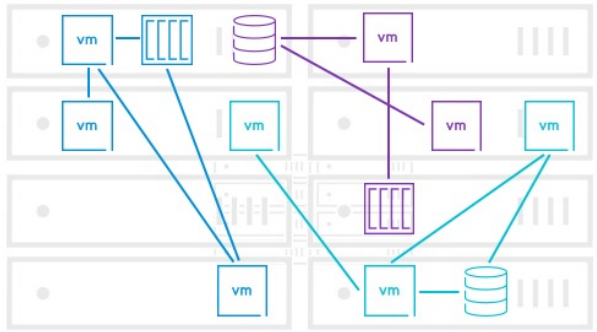
1. Src: [Any] to Dst: [Any] [TELNET, FTP, SMBv1, TLSv1] Action: Drop

BEFORE *AFTER*



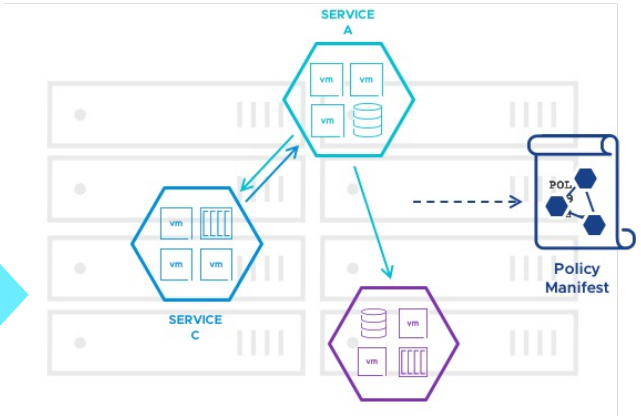
VMware Firewall

Real-Time Flow Visibility and Firewall Planning with Security Intelligence



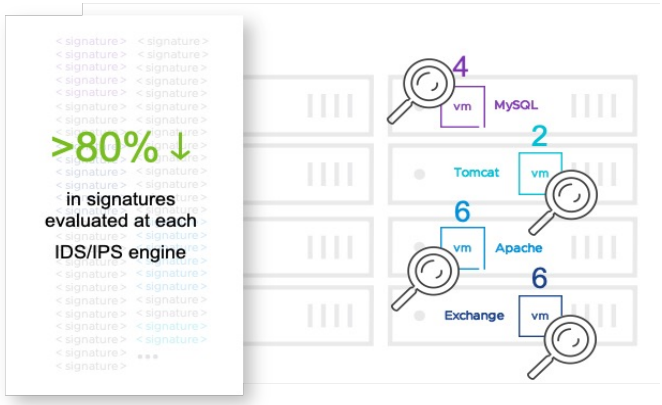
Real Time Flow Visibility

Complete visibility into every flow, every process, across all workloads



Application Grouping

Create application groups and create dependency maps



Policy Formulation

Recommend granular policies for segmentation purposes

admin

Home | Networking | Security | Inventory | Plan & Troubleshoot | System

POLICY MANAGER

Security | Application | Ecomm Store | Apply Filter | CLEAR

Flows: Unprotected | Blocked

Last 24h

Start New Recommendation

For a selected set of entities (VM Groups, Containers Groups or Baremetal), recommend DFW Rules for East-West traffic which can be validated and published.Recommended rules will consist of new Groups, Services and Context Profiles.

Recommendation Name: Ecomm Store Policy Recommendation

Description: Enter Description

Selected Entities in S ... ner Groups

Advanced Option

Time Range

Today

Current Selection: **Last 24 hours (Default)**

Tags: Enter one or more tags

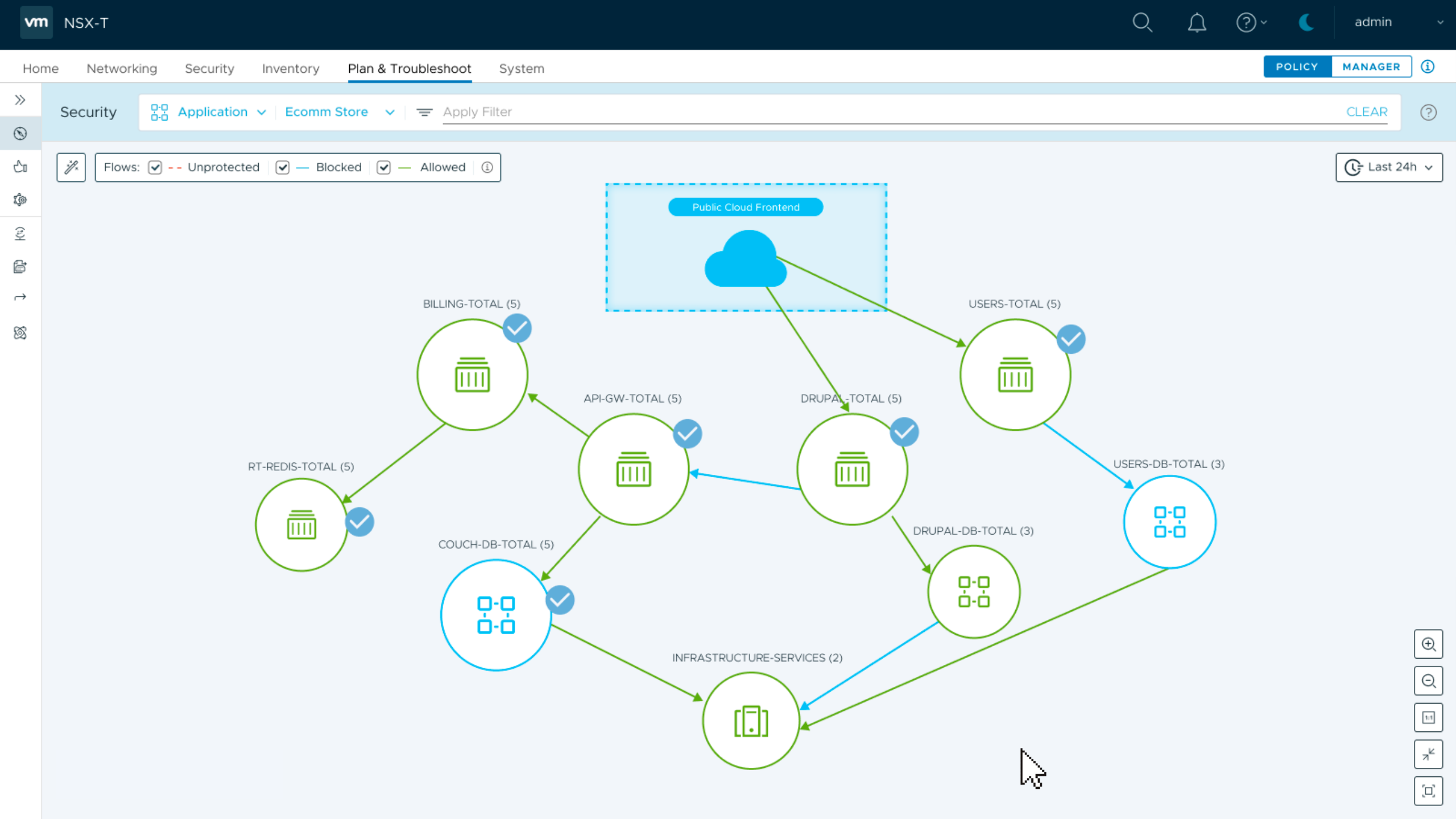
Recommendations Discovery in progress...

Recommendations Discovery can take upto 30 to 60 minutes. The discovery status can be tracked from the 'Recommendations' tab.

CANCEL | START DISCOVERY

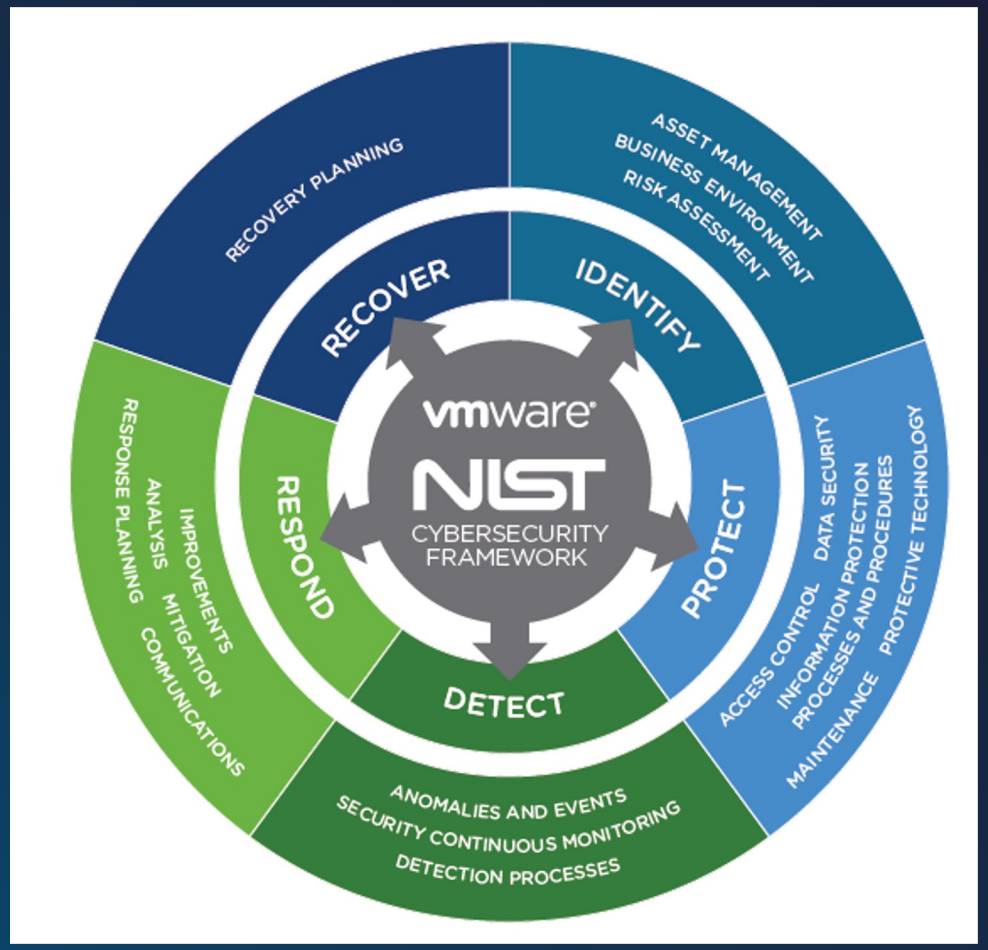
RT-REDIS-TOTAL (5)

SERS-DB-TOTAL (3)


NSX-T
admin
Home
Networking
Security
Inventory
Plan & Troubleshoot
System
POLICY
MANAGER
Security
Application
Ecomm Store
Apply Filter
CLEAR
Flows:
Unprotected
Blocked
Allowed
Last 24h
Public Cloud Frontend
BILLING-TOTAL (5)
USERS-TOTAL (5)
API-GW-TOTAL (5)
DRUPAL-TOTAL (5)
RT-REDIS-TOTAL (5)
USERS-DB-TOTAL (3)
DRUPAL-DB-TOTAL (3)
COUCH-DB-TOTAL (5)
INFRASTRUCTURE-SERVICES (2)

VMware Firewall and Advanced Threat Prevention

Mapping to NIST Cyber Security Framework



- A risk-based framework that provides a catalog of security controls for organizations to secure their systems.
- A comprehensive catalog of security and privacy controls applicable for Telecom sector.
- A foundation that allows all stakeholders to understand the organization's cyber risk.

VMware Firewall and Advanced Threat Prevention

Mapping to NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
			VMware Cloud Disaster Recovery →	
NSX Security →				
Baseline Network Environment	Network Segmentations	Signature-based & behavior-based detection (Network)	Network Quarantine	Validation of recovery points
High Value Assets Tagging	IDS/IPS/Deep Packet Inspection	Signal Correlation Across Detectors	Network Resets	File and folder-level recovery
Flow Visualization	Attack Surface Reduction	Sandbox/Malware Detection	Allow/Deny	Delta-based Failback
DR Plan Config, Test, Check	Micro-segmentation	Network Anomaly	Failover to Isolated Recovery Environment	Review, Audit & Remediate
Application Dependency Mapping	Malware Prevention		Identify restore point candidates	

NSX Security

VMware Cloud DR

Thank You

vmware by Broadcom