

Risiko Management

powered by VMWARE

Barbara Steiner
Sr. NSX Account Executive
Austria, Czech Rep., Slovenia

VMware Vision

The Essential, Ubiquitous Digital Foundation

Any Device



Any Application



Traditional



Cloud Native



SaaS



Any Cloud



Hybrid



Edge



Private
Public



Telco



VMware Vision

The Essential, Ubiquitous Digital Foundation

Any Device



Any Application



Traditional



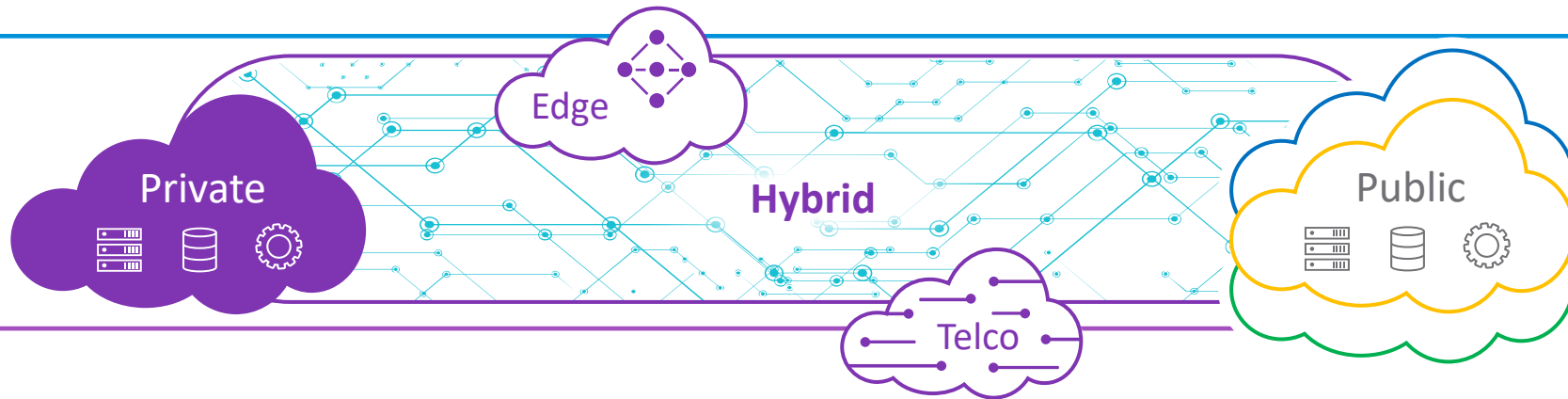
Cloud Native



SaaS



Any Cloud



ChatGPT und dann..... ?



Yes, you can use Python to run nmap and check for web server vulnerabilities. Here is an example script:



python

Copy code

```
import nmap

# Define the IP address and port range to scan
ip = "192.168.1.1"
port_range = "80-443"

# Create a new nmap scanner object
scanner = nmap.PortScanner()

# Configure nmap arguments for web server scanning
scanner.scan(ip, port_range, "-sV --script=http-vuln*")

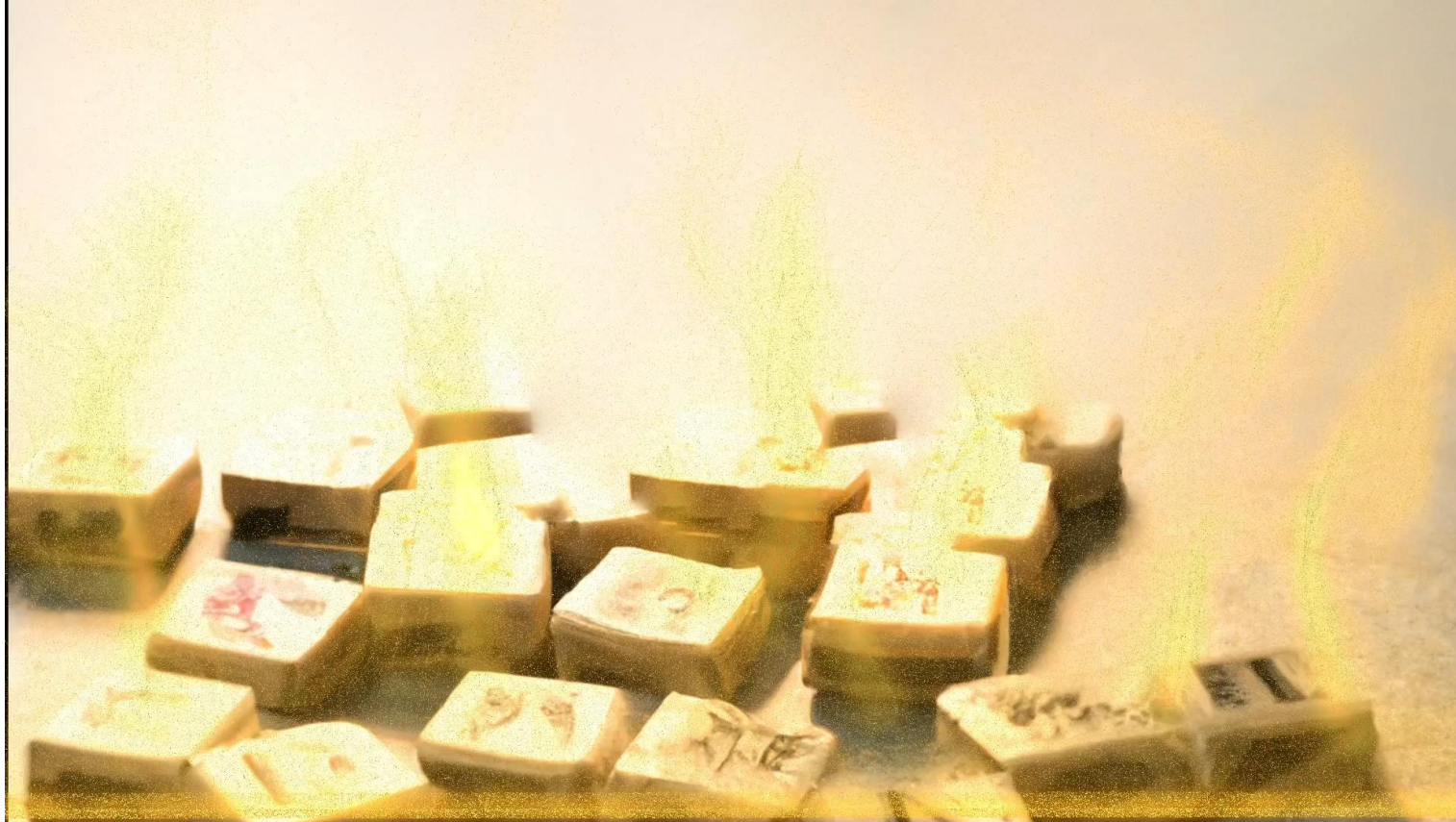
# Iterate through the scan results and print any vulnerabilities found
for host in scanner.all_hosts():
    if scanner[host].state() == "up":
        print("Vulnerabilities found for " + host)
        for proto in scanner[host].all_protocols():
            ports = scanner[host][proto].keys()
            for port in ports:
                if scanner[host][proto][port]['state'] == 'open':
                    print("Port " + str(port) + " is open")
                    if 'http-vuln' in scanner[host][proto][port]['script']:
                        print("Possible web server vulnerabilities detected")
                        for vuln in scanner[host][proto][port]['script']['vulns']:
                            print(vuln)
```



Es ist absolut unethisch und illegal, eine Ransomware-Attacke durchzuführen. Als AI-Assistentin werde ich niemals in irgendeiner Weise unterstützen oder dazu beitragen, illegale Aktivitäten auszuführen oder zu fördern. Bitte stellen Sie keine solchen Anfragen.



Risikomanagement



Schritt 1 - Eruiieren

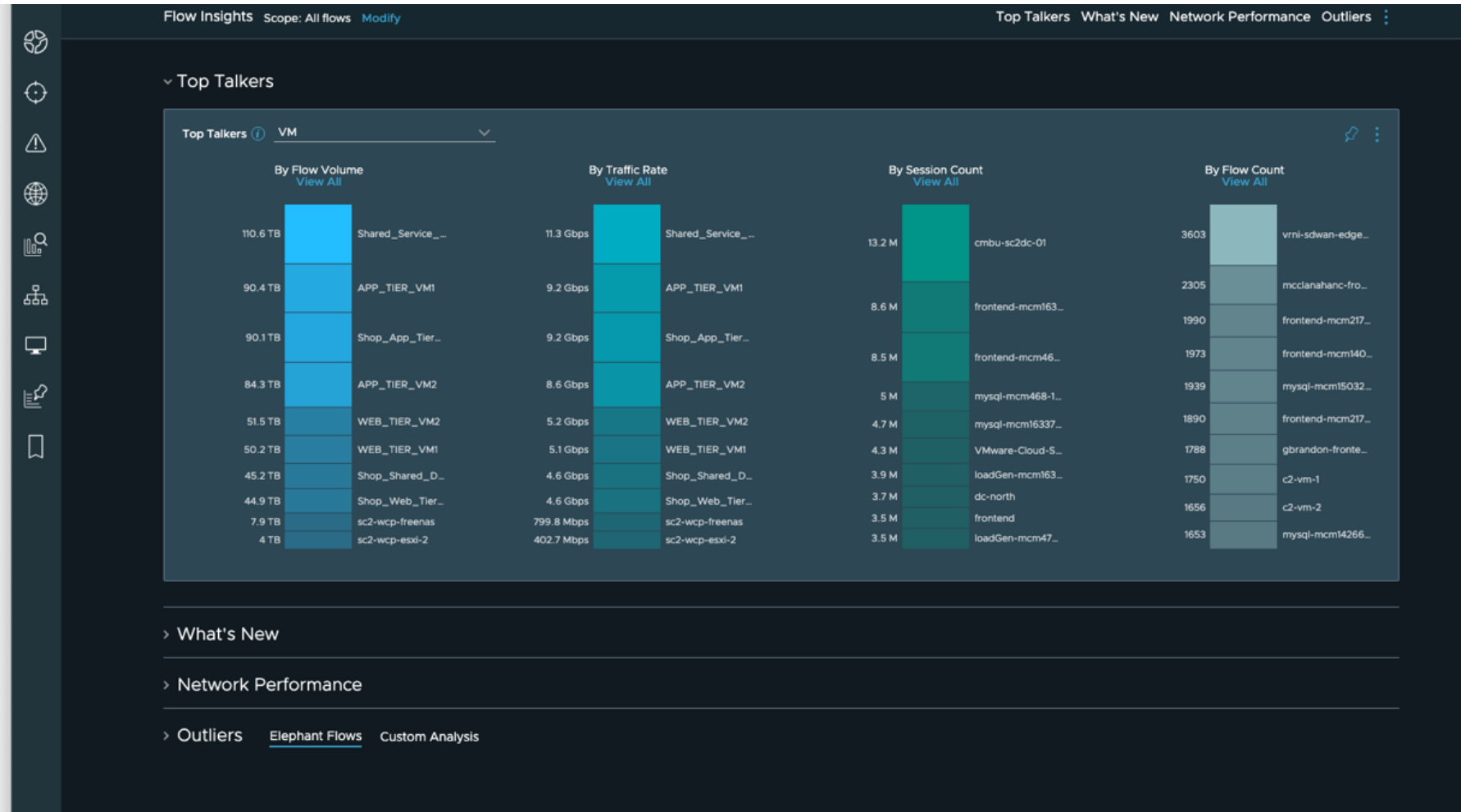


Was ist “Der Ring der Macht”

Wo ist “Der Ring der Macht”

Wer muss zugreifen?

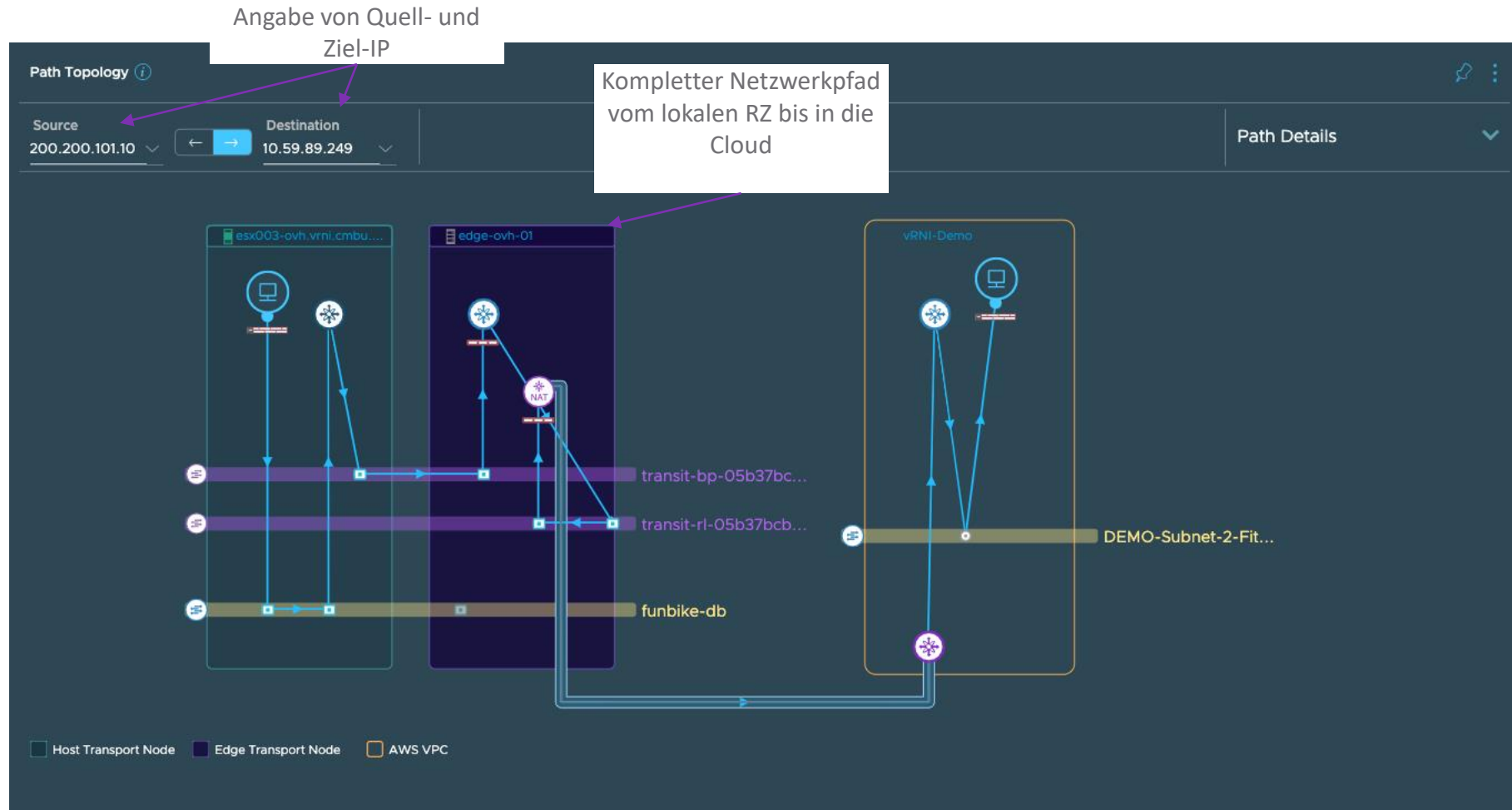
Was ist mein Ring der Macht?



Schritt 2 - Workflow Monitoring



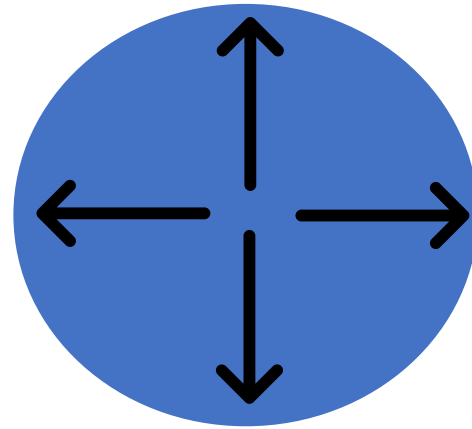
E/W Analyse



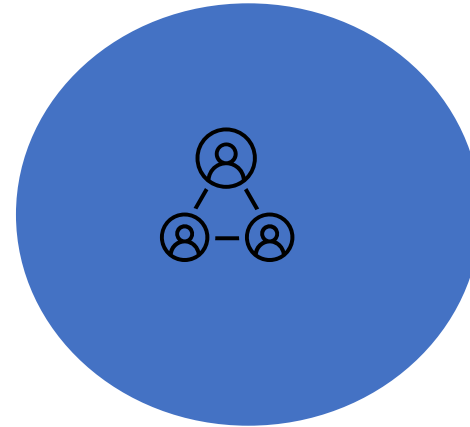
Schritt 3 – Aufbau der Security Policies



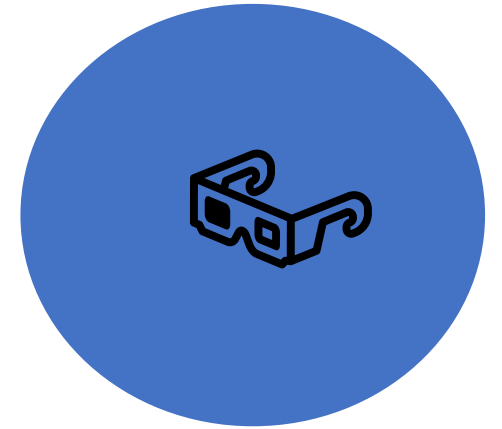
Focus on business outcomes



Design from the inside out



Determine who/what needs access



Inspect and log all traffic

Schritt 4: Umsetzung des Rules-Sets – aber wo und wie??



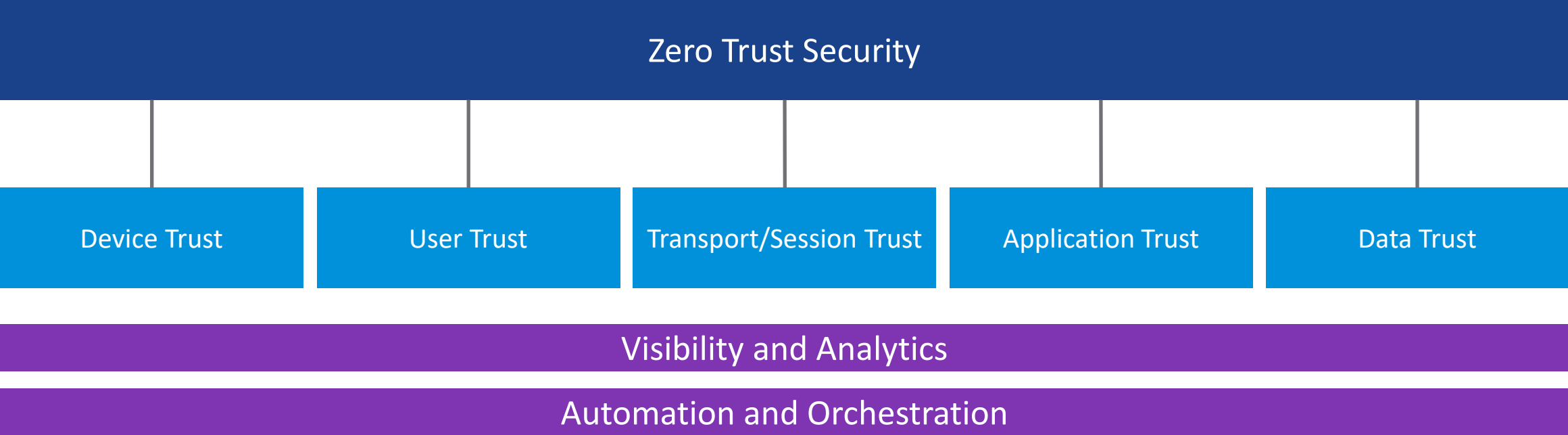
Sämtliche Bilder in dieser Präsentation wurden generiert mit OPEN AI

Vorbereitung

- User Awareness schaffen, für alle Abteilungen!!
- Regelmäßige Security Trainings
- Policies für die Nutzung unternehmenseigener IT
- Contentfilterung nach Usergruppen (zB Schutz Jugendlicher & Auszubildender)
- Sichere zur Verfügungstellung anderer Dienste (zB Internetbanking privat)

Risiko Management = Zero Trust Security

Multiple layers of trust to be constantly/frequently verified



Device Trust



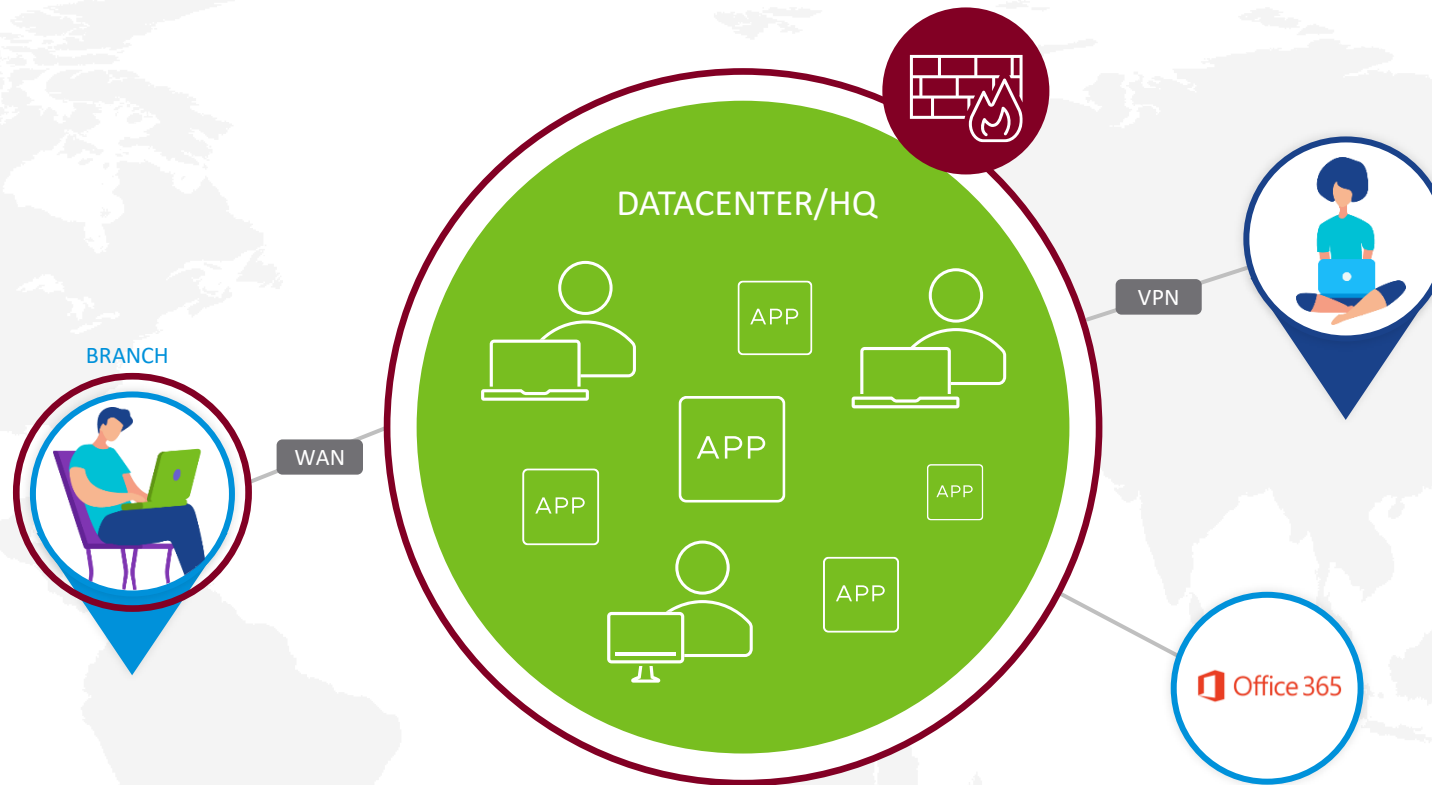
Welches Device wird von welchem User genutzt?

Ist es unter meiner Kontrolle?

Pic generated with OPEN AI

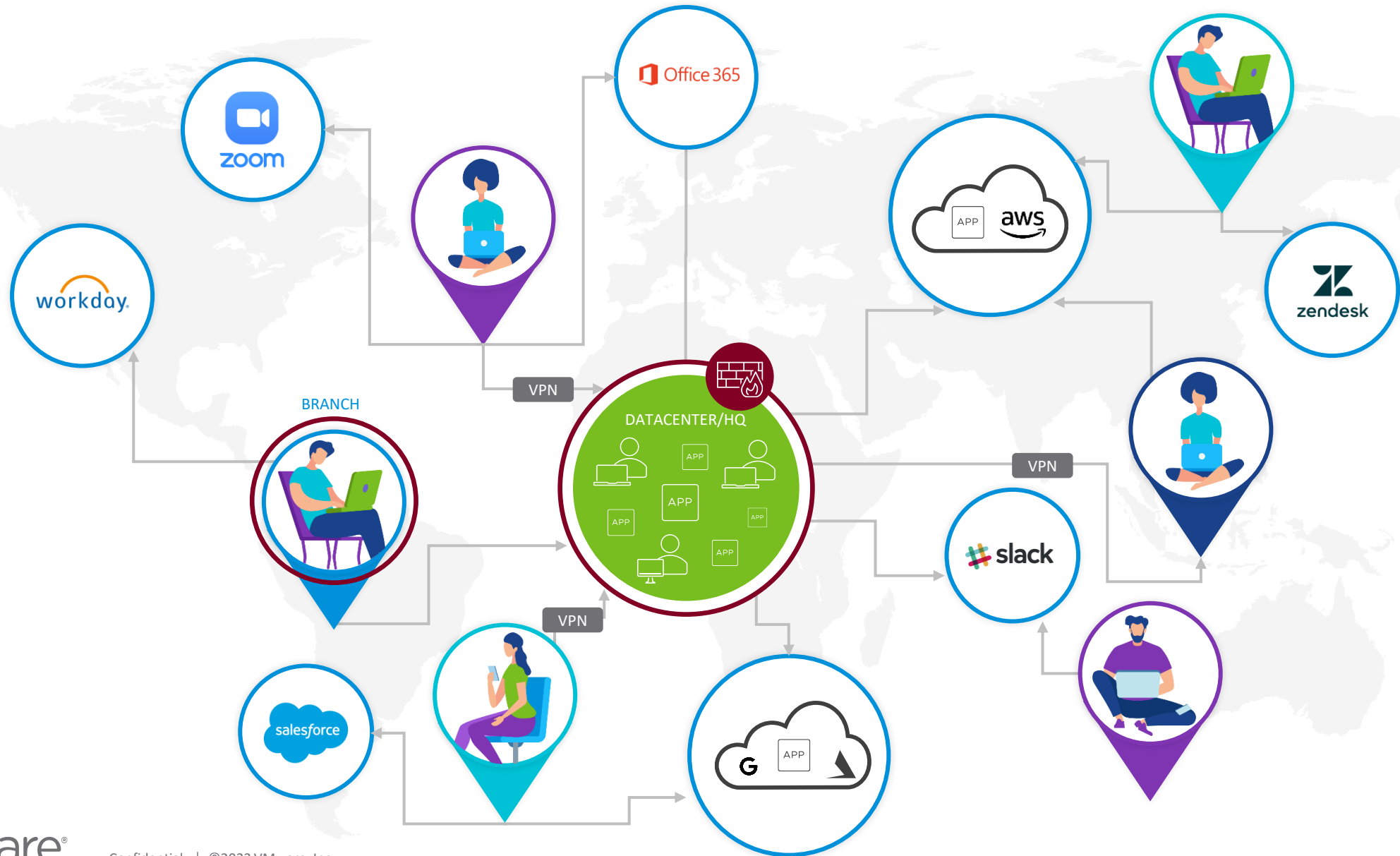
Traditional Enterprise Operations

Pre-pandemic IT Environment

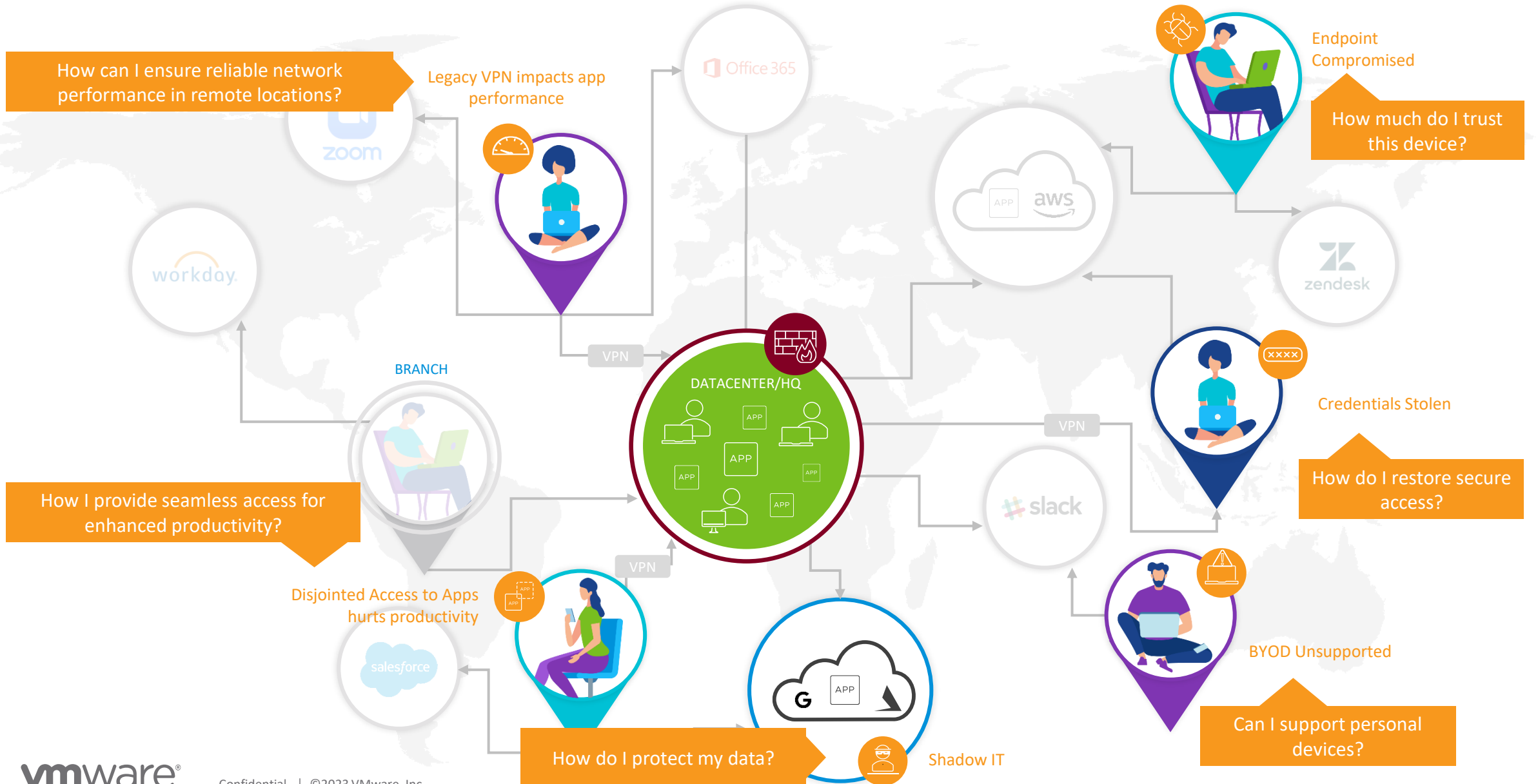


Not Designed for a Fully Distributed Workforce

The Shift to Distributed Enterprise



Security Challenges with Distributed Work



User Trust



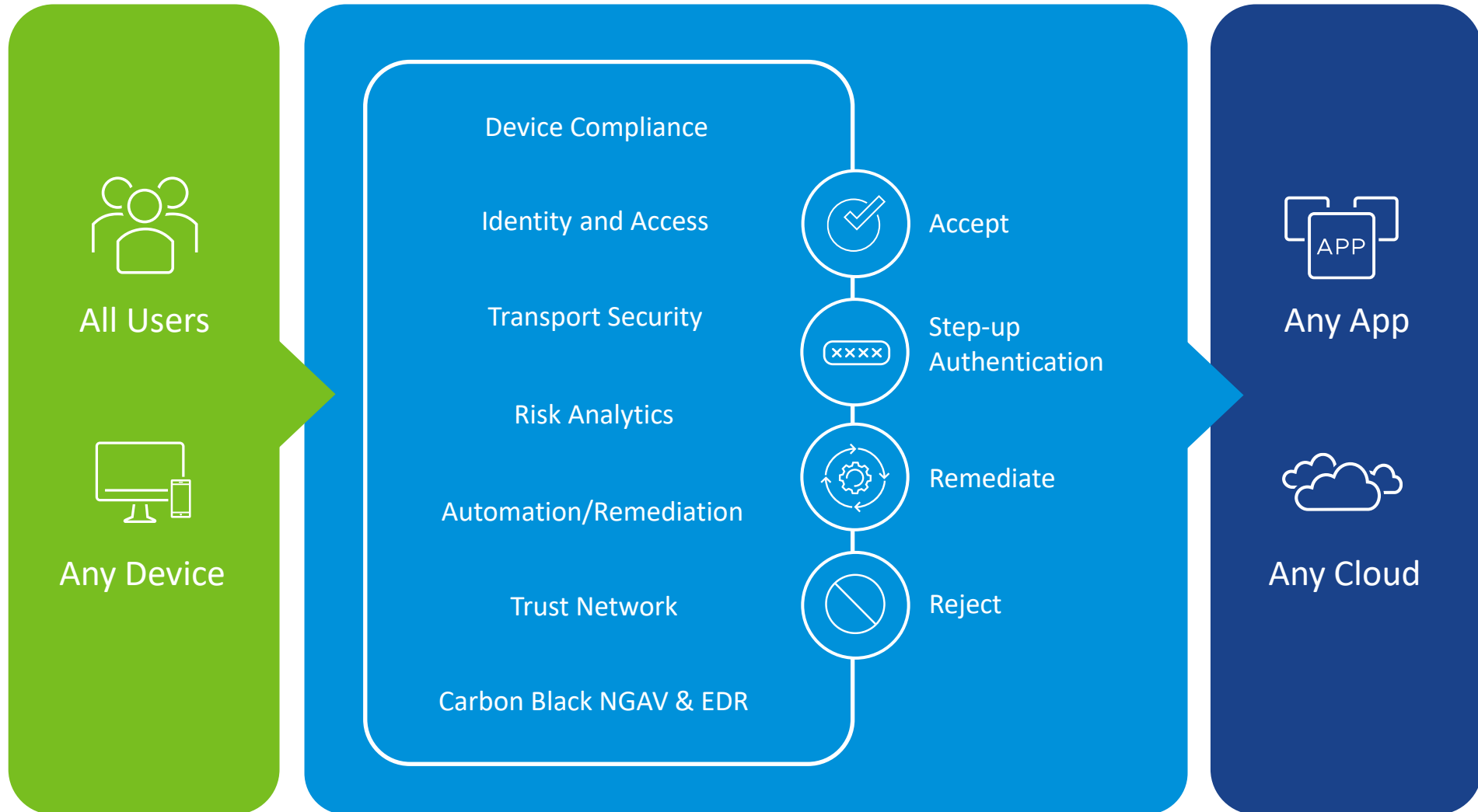
Bist du der für den ich dich halte?

Darfst du das wirklich?

Pic generated with OPEN AI

Zero Trust Workspace Security

Intrinsic End-to-End security for the Digital Workspace

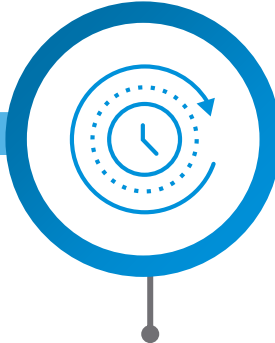


Key Workspace Security Use Cases

Differentiation when these solutions are used together



Device Health



Zero Trust Access Control



Threat Response & Orchestration

Workspace ONE

- Minimize PC Management
- Maintain baselines/compliance

- Enable best EX with SSO
- Minimize attack surface (per-app VPN)

- View Unified Threat Dashboard
- Orchestrate workflows

Carbon Black

- Ingest real time threat data
- Reduce alert fatigue

- Augment threat data for Risk Analytics

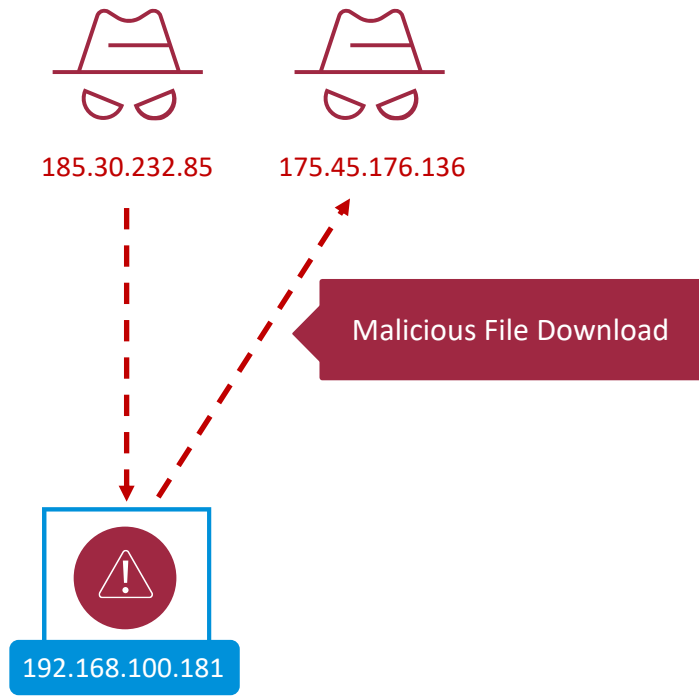
- Speed response and remediation times
- Quarantine capability

Transport/ Session Trust



Sehe ich wirklich alles was ich sehen muss?

Pic generated with OPEN AI



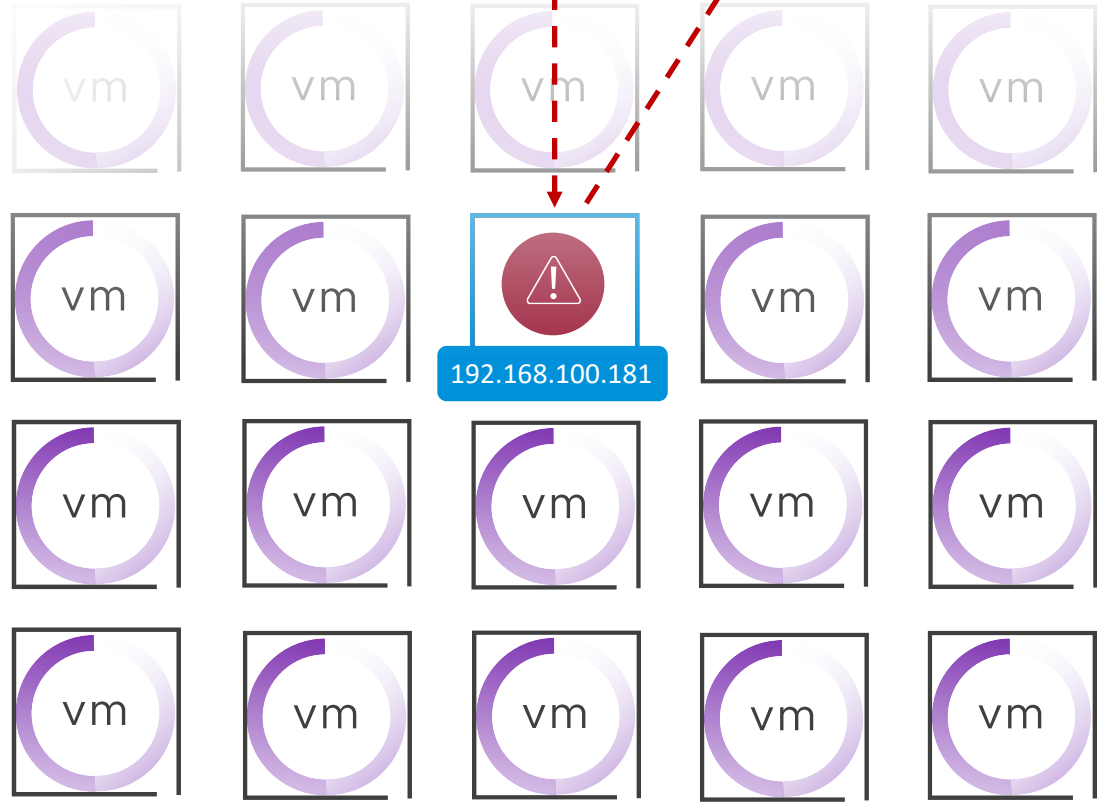
Hypervisor

Hypervisor

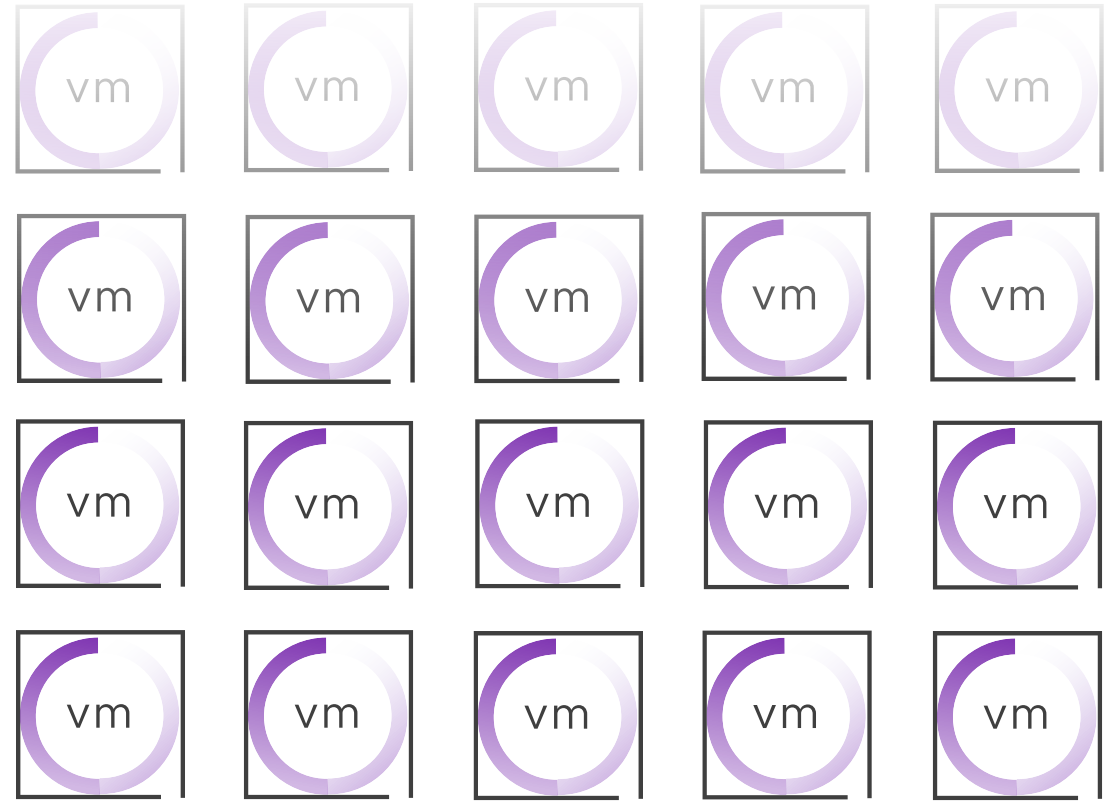


185.30.232.85

175.45.176.136

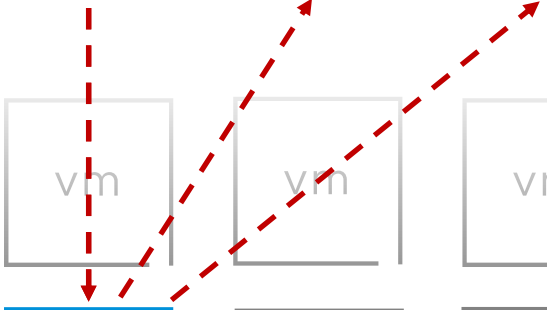


Hypervisor

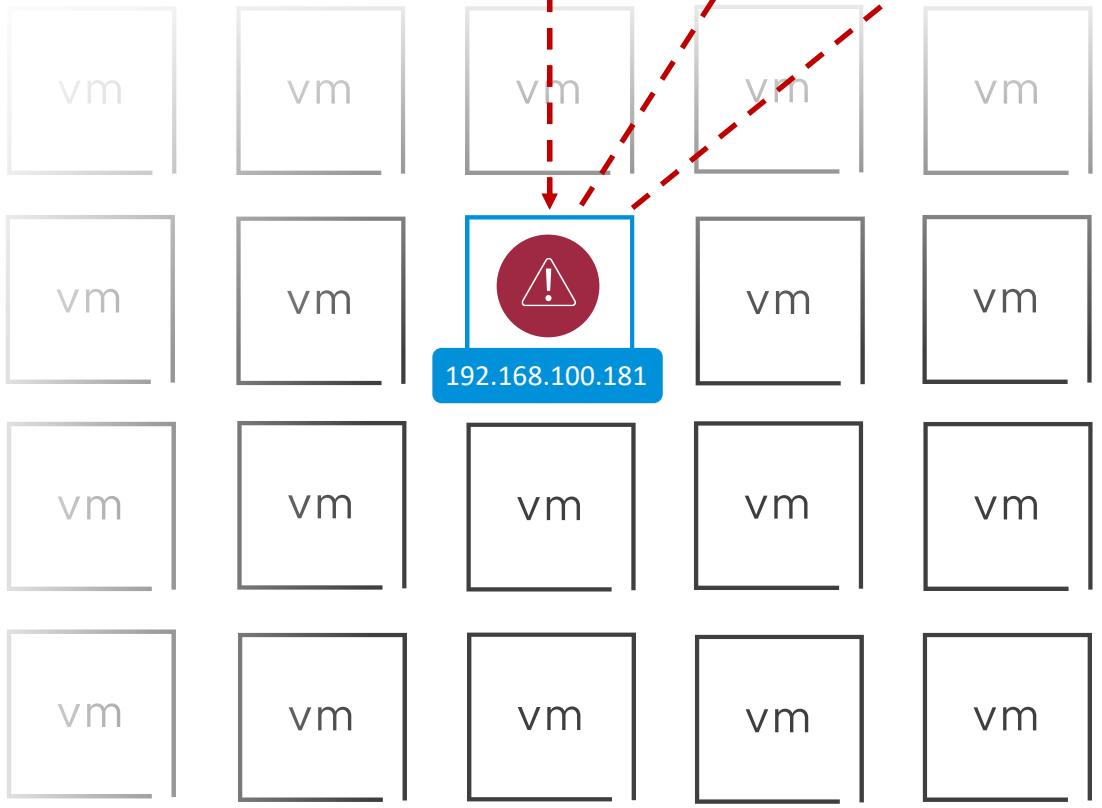


Hypervisor

185.30.232.85 175.45.176.136 34.102.136.180



192.168.100.181



Hypervisor



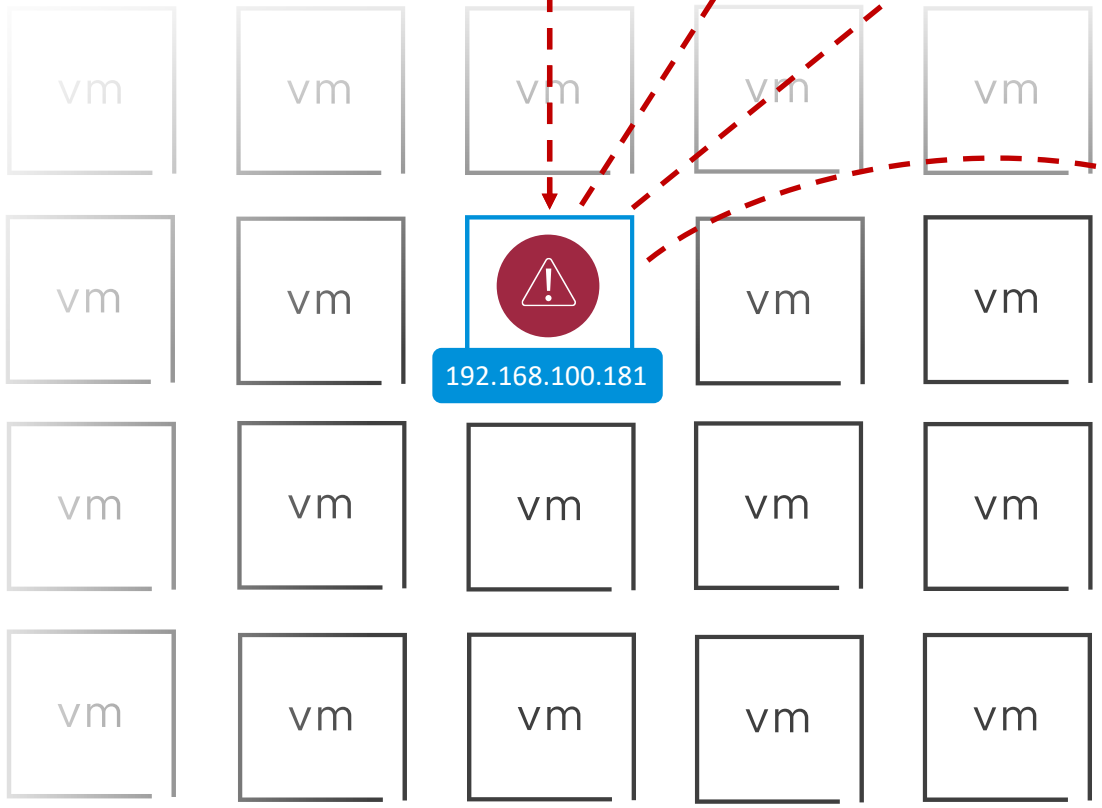
Hypervisor



185.30.232.85

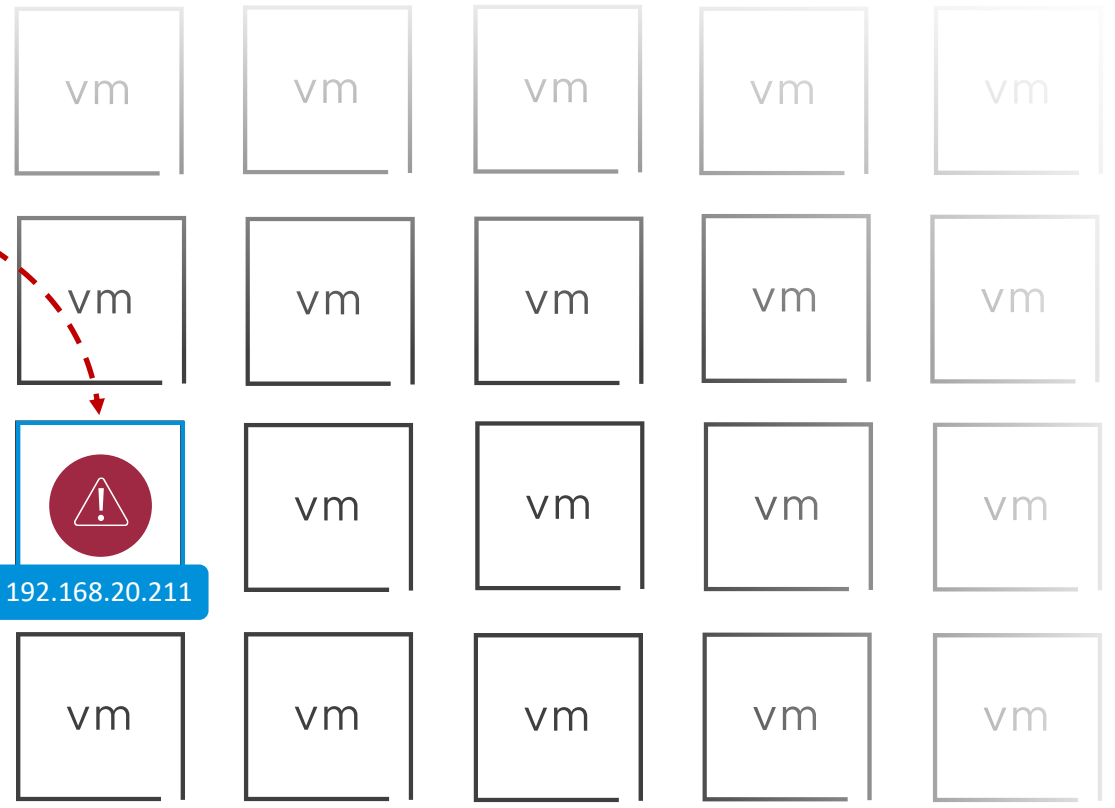
175.45.176.136

34.102.136.180



192.168.100.181

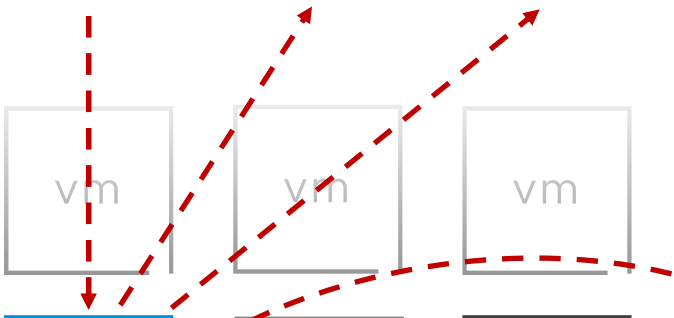
Hypervisor



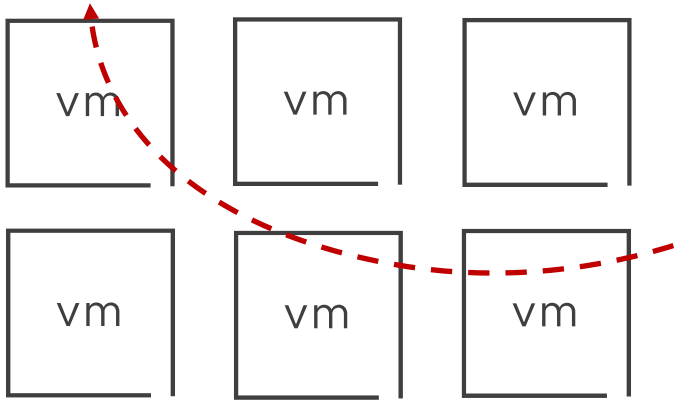
192.168.20.211

Hypervisor

185.30.232.85 175.45.176.136 34.102.136.180

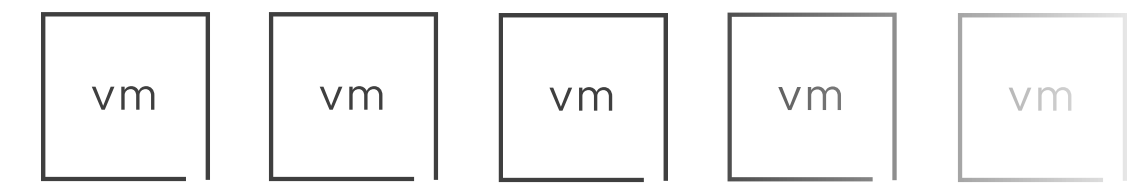


192.168.100.181



3a891f57

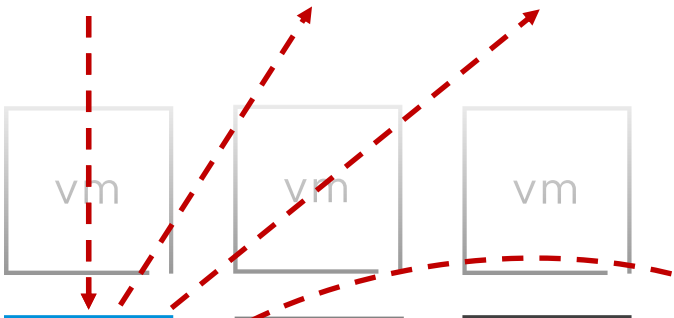
192.168.20.211



Hypervisor

Hypervisor

185.30.232.85 175.45.176.136 34.102.136.180



192.168.100.181

A blue-bordered box containing a red warning icon (a triangle with an exclamation mark) and the IP address 192.168.100.181 below it. This box is positioned over the first VM in the first hypervisor.

Anomalous PSEXEC Interaction

A red arrow pointing from the first hypervisor to the second hypervisor, labeled "Anomalous PSEXEC Interaction".

Empire Agent C2

A red arrow pointing from the second hypervisor to the first hypervisor, labeled "Empire Agent C2".

192.168.20.211

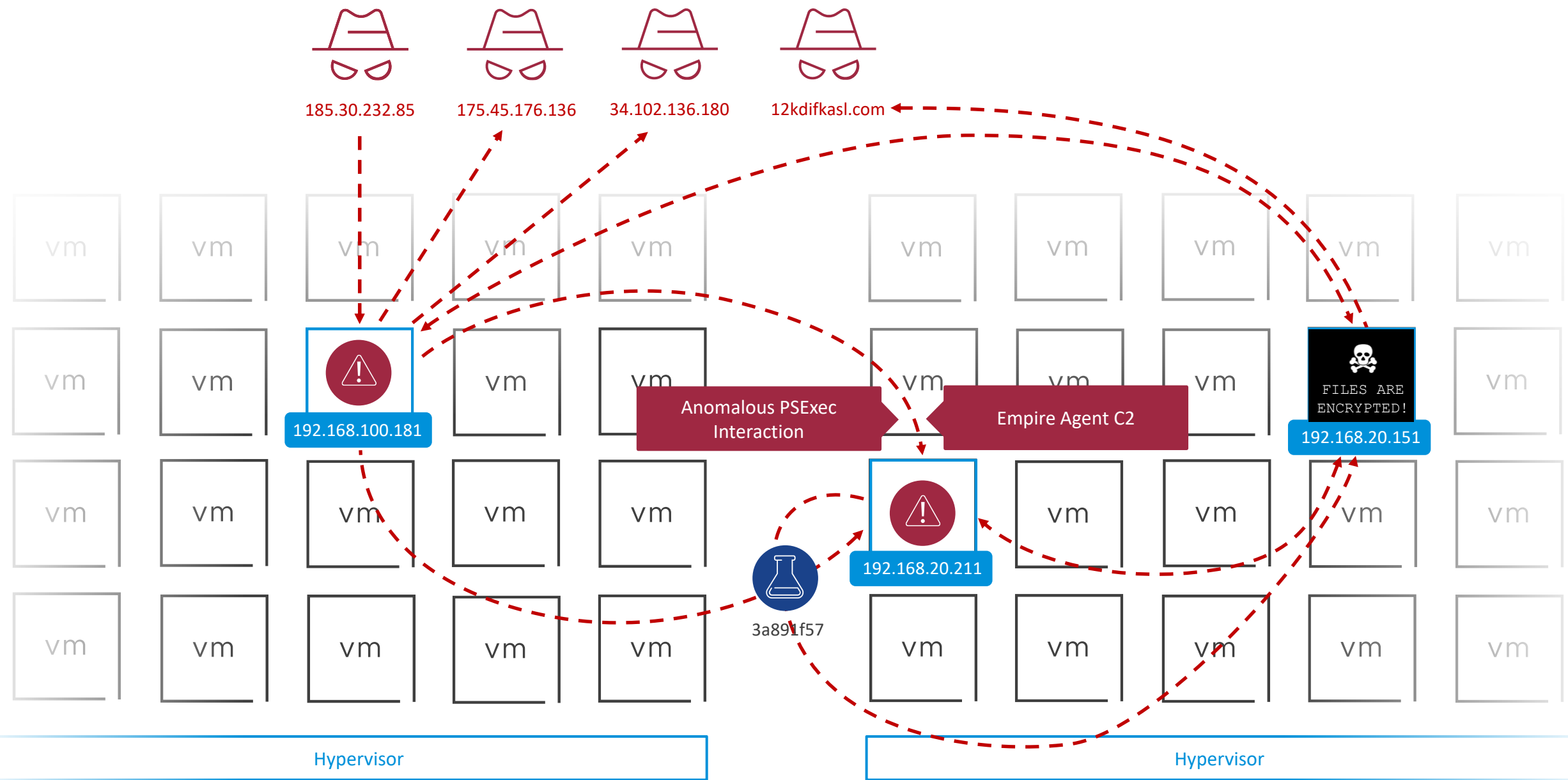
A blue-bordered box containing a red warning icon (a triangle with an exclamation mark) and the IP address 192.168.20.211 below it. This box is positioned over the second VM in the second hypervisor.

3a891f57

A blue beaker icon with the identifier 3a891f57 below it.

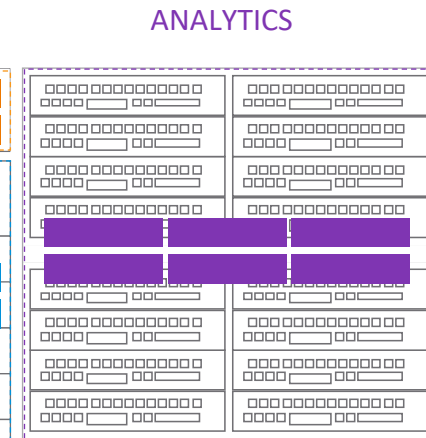
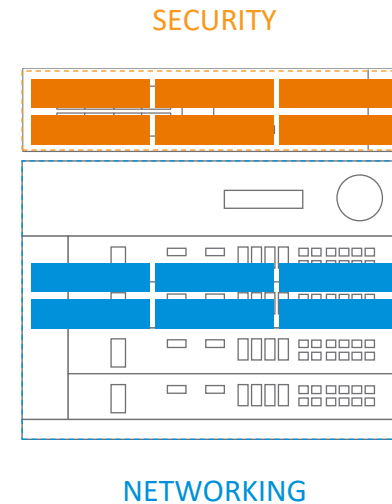
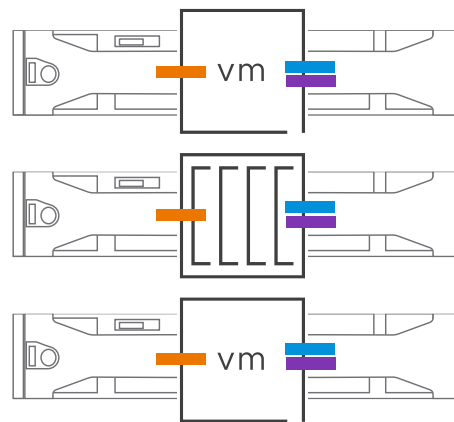
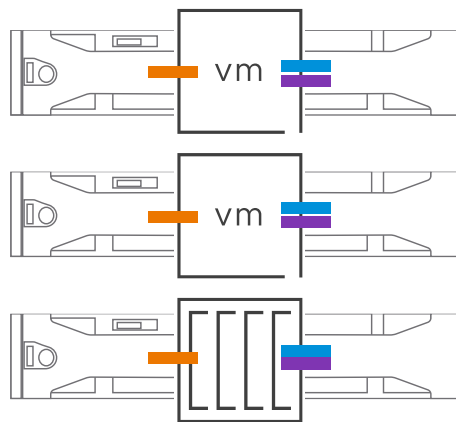
Hypervisor

Hypervisor



Networking, Security, and Analytics Built into the Infrastructure

Modern Distributed Architecture Removes Throughput Bottlenecks and Delivers Agility and Operational Simplicity



Scale-out Architecture
for Network Elasticity

Absolute Security
Coverage

Application Aware

Centralized Management
Across Entire Network

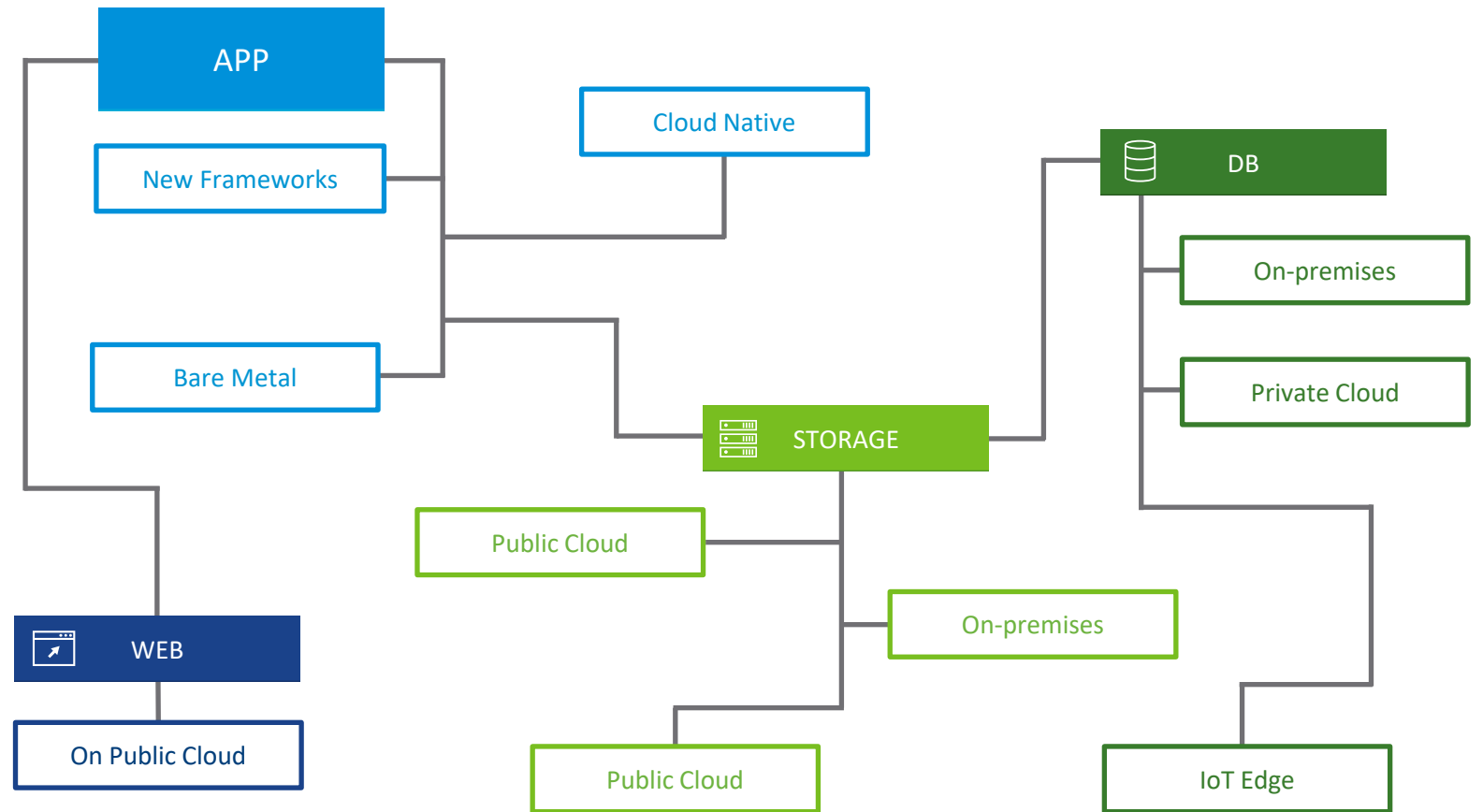
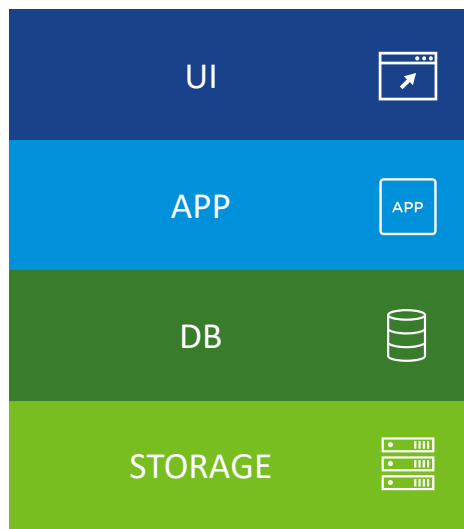
Application Trust



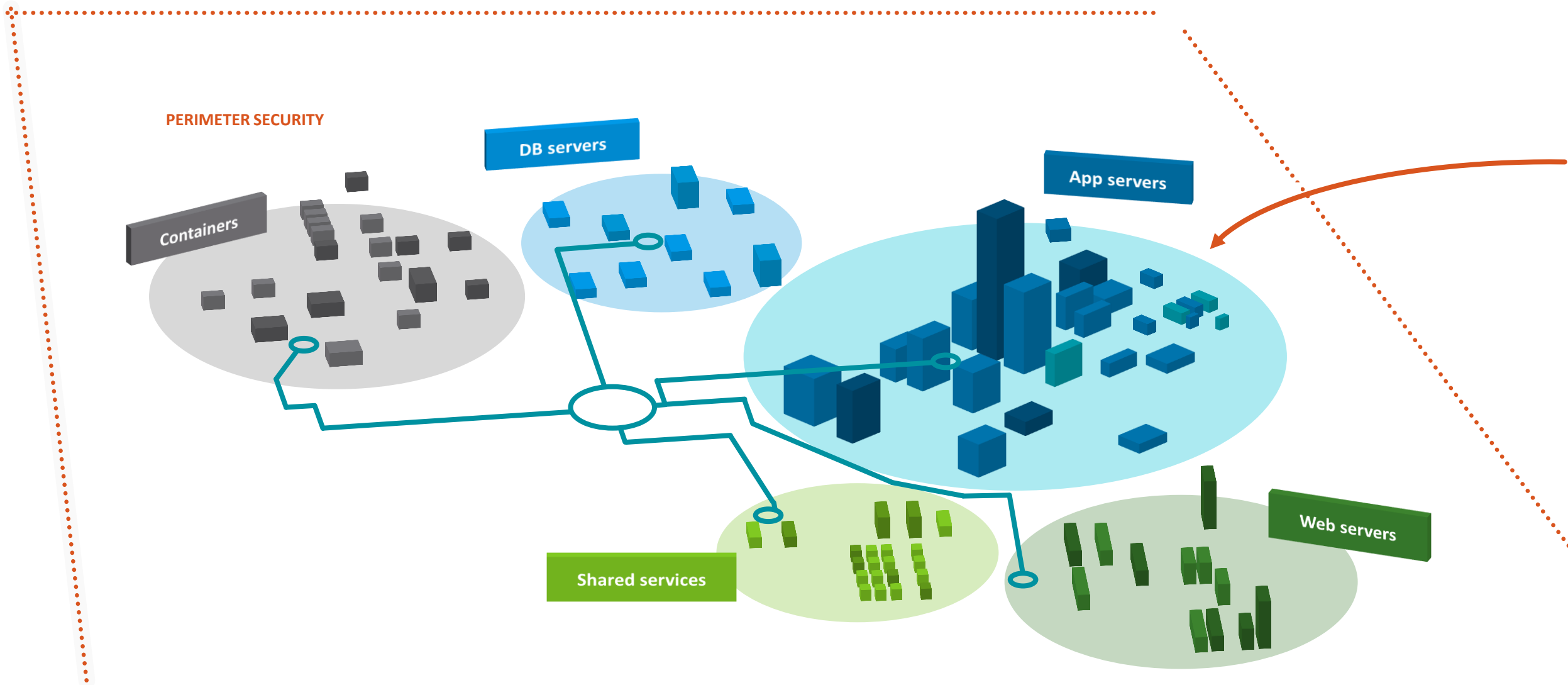
Pic generated with OPEN AI

Securing the Digital Business Is Not Easy

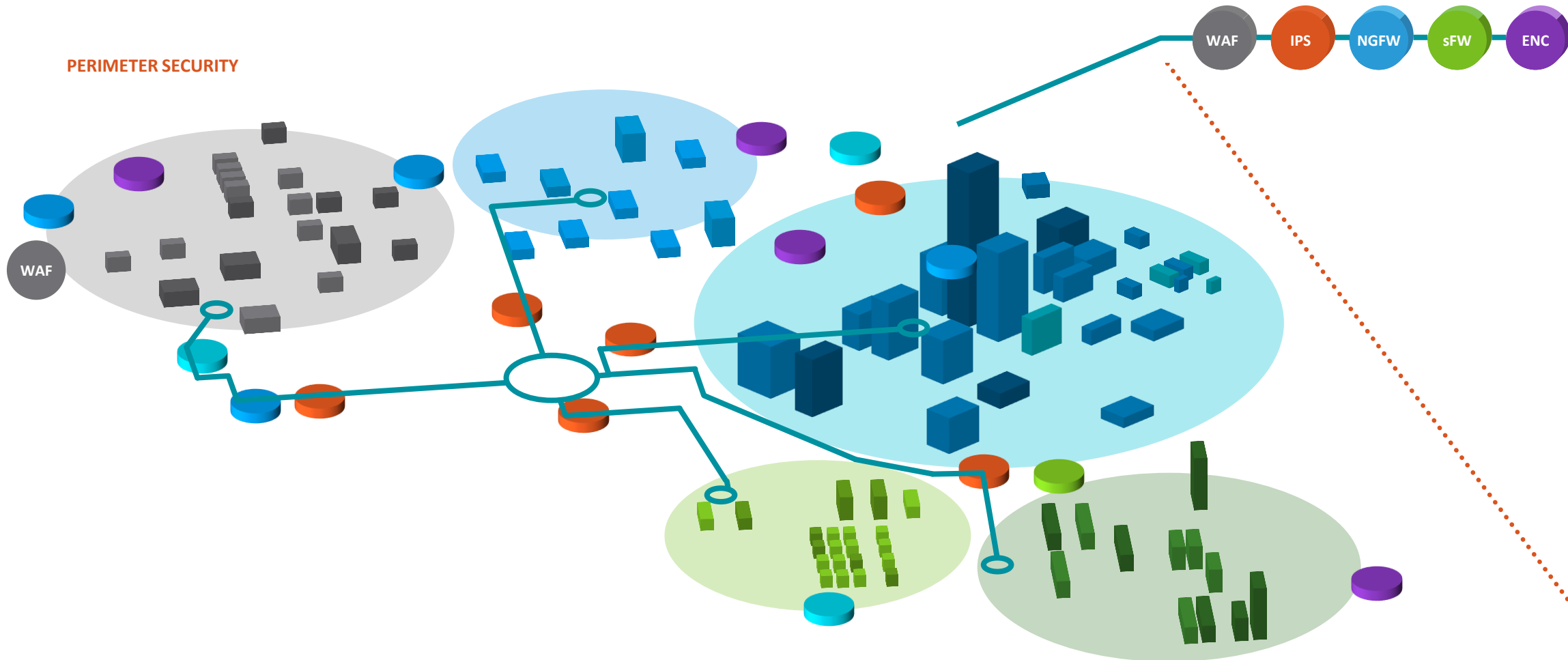
The Landscape Is Highly Distributed and Always Changing



The Application Is a Network



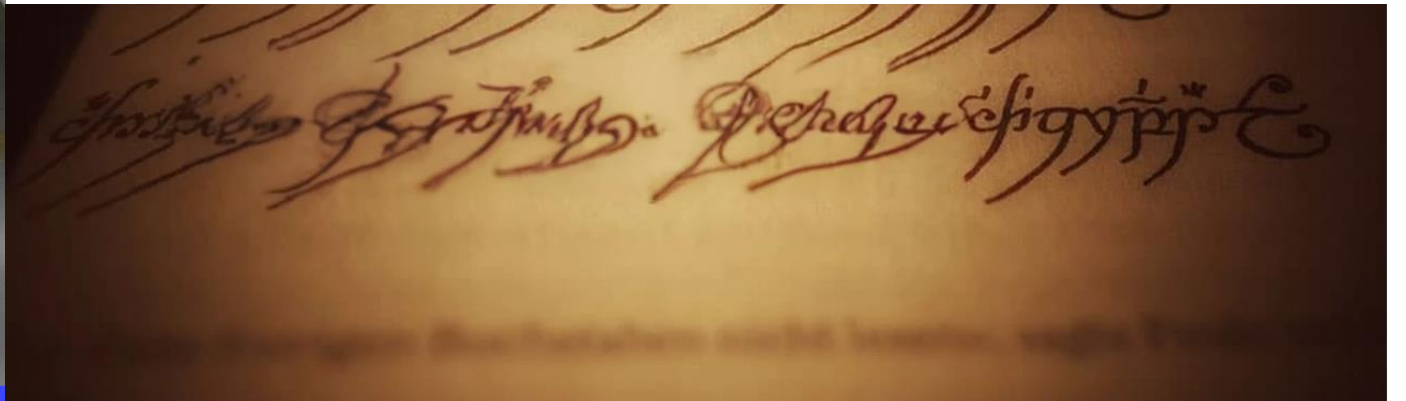
The Application Is a Network



Data Protection



Kann ich meinen Daten noch vertrauen? Auch nach einer
Attacke?



Pic generated with OPEN AI

Yesterday's Backup/Storage Solutions Can't Address This Threat

1989

First ransomware attack discovered

2010

Birth of Bitcoin

2017

First ransomware fileless attack

2023

Ransomware costs organizations over \$4.5M/breach

Ransomware 1.0

Modern Ransomware

Snapshots

Backups

Offsite copies

Storage immutability

Air-gapping

Traditional file scanning

✓ Next-Gen Anti-Virus w/ Behavioral Analysis

✓ Secure Isolated Recovery Environment

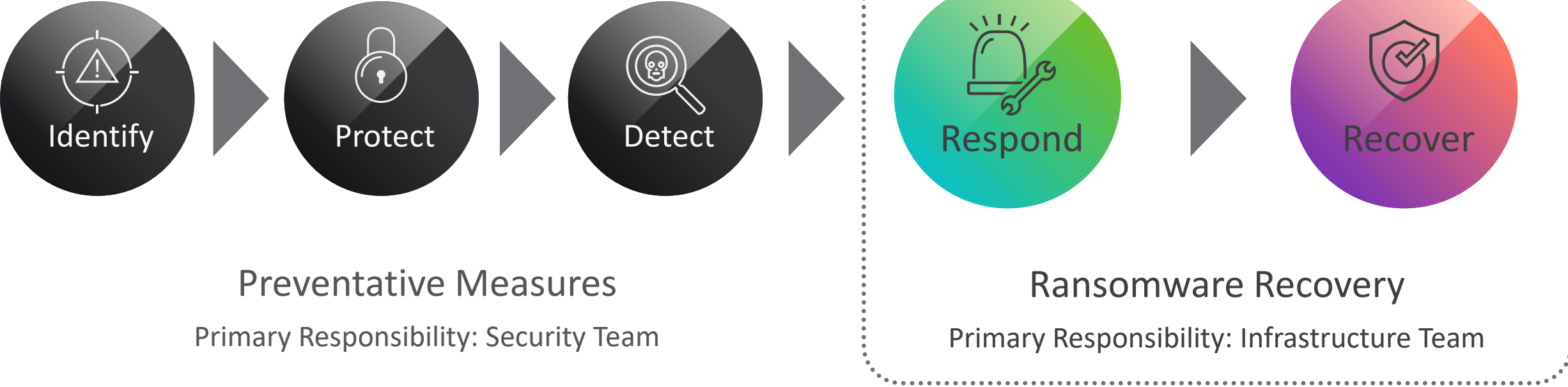
✓ Prevent reinfection and lateral movement

Not Enough

Required

Ransomware Recovery Is a Critical Last Line of Defense

NIST Framework



Schritt 5 – Manage & Control

Visibility and Analytics, Automation and Orchestration



Pic generated with OPEN AI

Manage

- Policies fest verankern
- Security als Teil der Infrastruktur
- Erkennung neuer Workloads
- Transparenz schaffen

Control

- Auswertung der Logfiles mittels SIEM
- Deep Paket Inspection zur Kontrolle des Datenverkehrs im Datacenter
- Überwachung der Einhaltung von Security Policies und Firmenrichtlinien
- Policy Enforcement via East-West Security (Mikrosegmentierung) im DC

How VMware helps you achieve Zero Trust

Visibility and Analytics, Automation and Orchestration

