Principal Cloud Security Architect

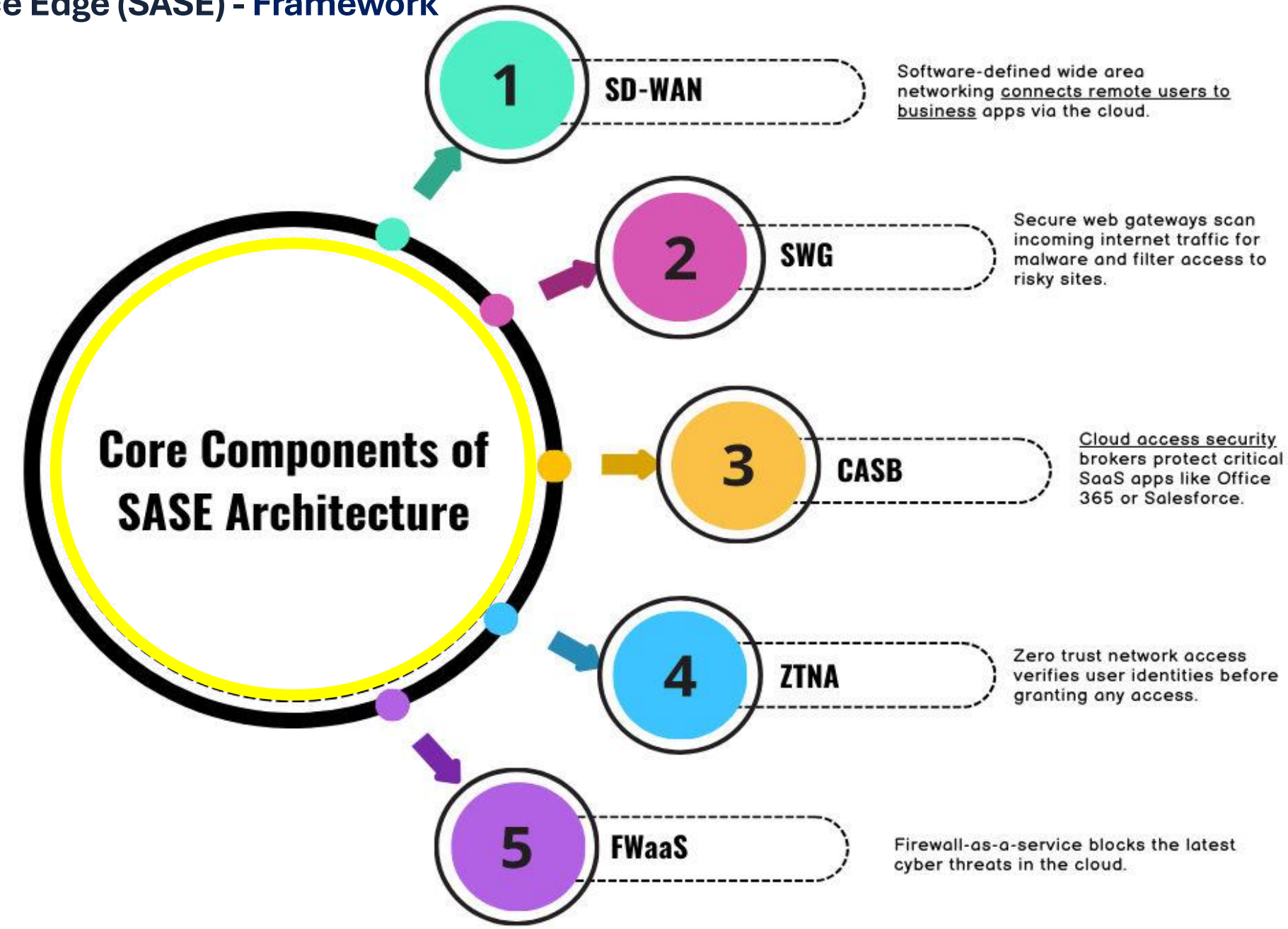
Secure Cloud Computing Strategy

Halliwell M. Longley
Sept. 16, 2025

Table of Contents

Secure Access Service Edge (SASE) - Framework

- The Secure Access Service Edge (SASE) framework is a security model that integrates software-defined wide area networking (SD-WAN) and Zero Trust security solutions into a unified, cloud-delivered platform.
- This framework aims to securely connect users, systems, endpoints, and remote networks to applications and resources, regardless of their location.

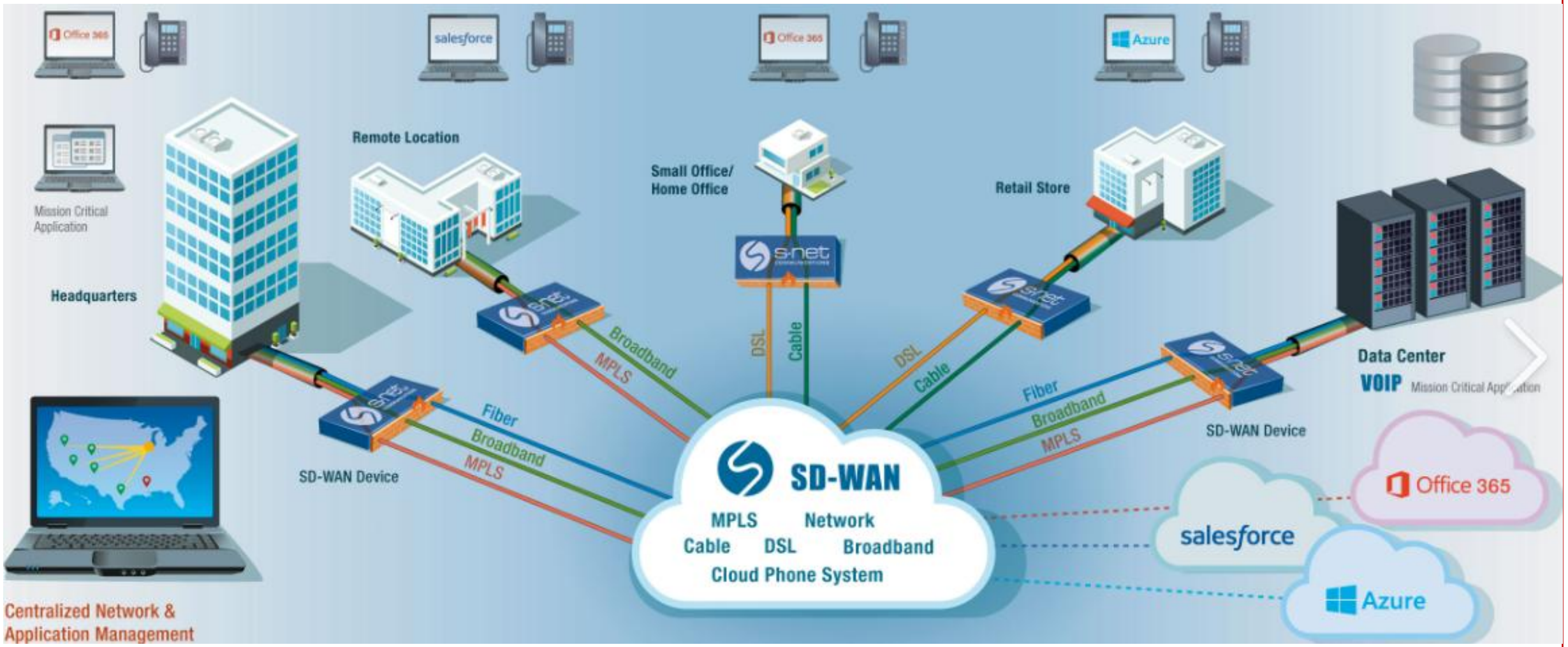


1 Software-Defined Wide Area Networking (SD-WAN) – Manage network traffic

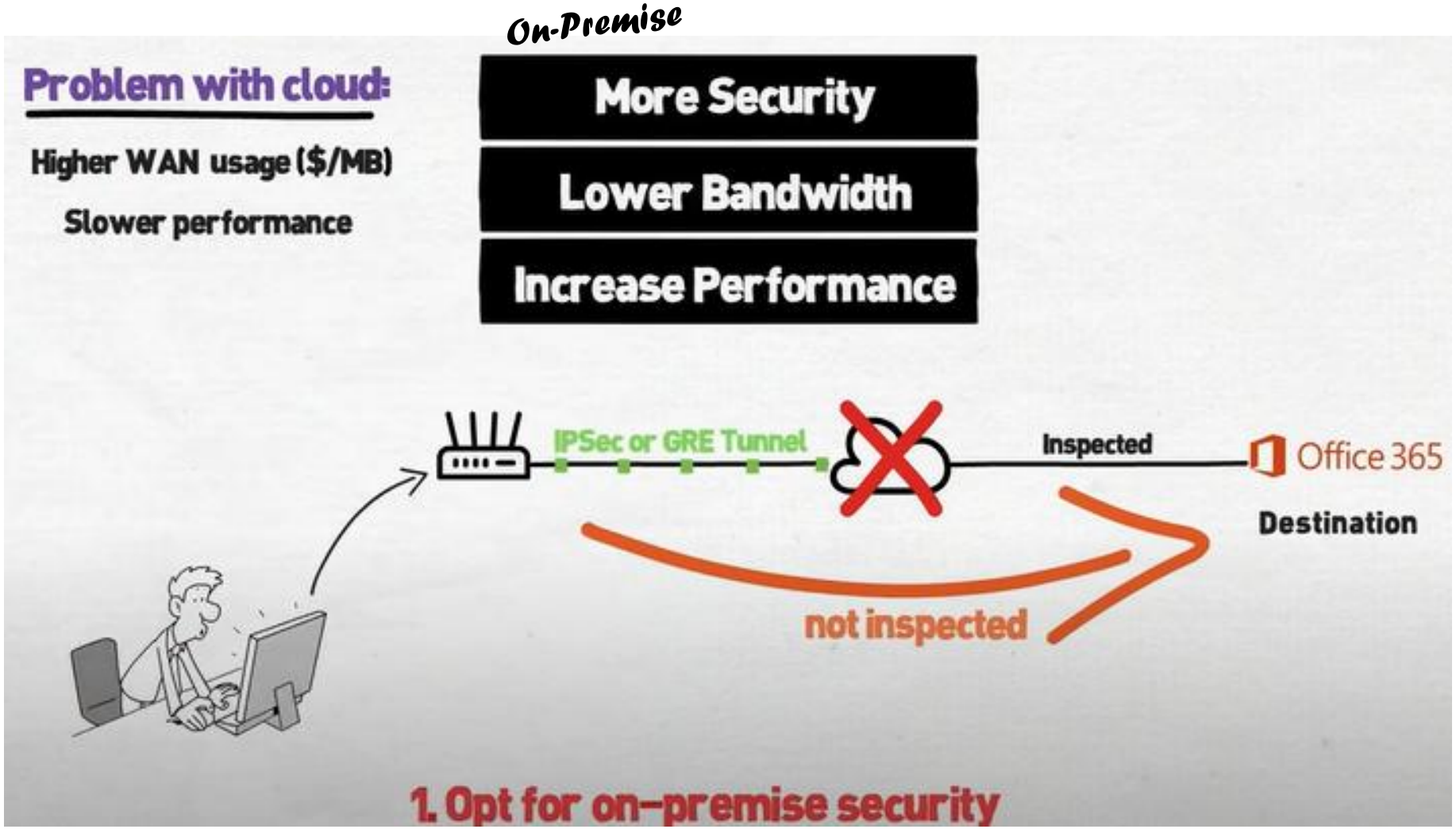
- **Software-Defined Wide Area Network (SD-WAN)** is a modern approach to managing and optimizing wide-area networks (WANs).
- Unlike traditional WANs, which rely on fixed, hardware-based configurations, SD-WAN uses software to intelligently route traffic across multiple connection types, such as MPLS, broadband, and LTE, based on real-time conditions and application requirements.
- SD-WAN provides a centralized interface for managing network traffic, enabling organizations to efficiently connect users to applications hosted in data centers, public clouds, or SaaS platforms.
- This approach addresses the limitations of traditional WANs, which struggle with the growing demands of cloud-centric environments.

YouTube Securing SD-WAN: 5 Considerations

1 Software-Defined Wide Area Networking (SD-WAN) – Device (Cloud or on-premise)



1 Software-Defined Wide Area Networking (SD-WAN) – On-premise security vs cloud



Top vendors

CISCO

JUNIPER NETWORKS

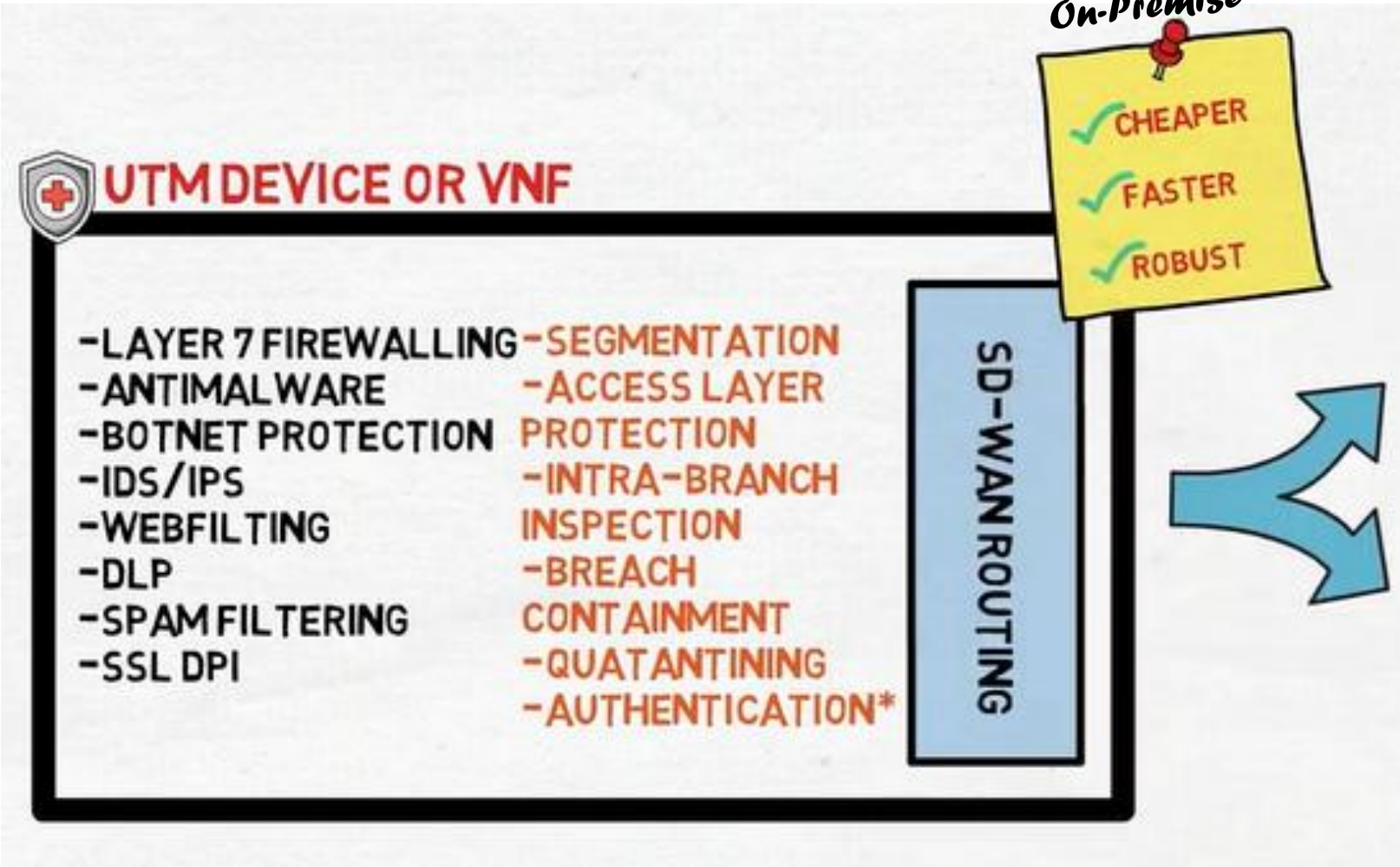
riverbed

FORTINET

YouTube Securing SD-WAN: 5 Considerations

1

Software-Defined Wide Area Networking (SD-WAN) – On-premise security vs cloud



YouTube Securing SD-WAN: 5 Considerations

2

Secure Web Gateway (SWG)

- A Secure Web Gateway (SWG) is a security solution that monitors and filters web traffic to block malware, phishing, and unauthorized data transfers.
- Positioned between users and the internet, SWGs enforce corporate policies, inspect encrypted traffic (HTTPS), and prevent access to malicious or non-compliant websites.
- With remote work and cloud adoption accelerating, SWGs have evolved from on-prem appliances to cloud-native services, integrating with broader security frameworks like SASE.
- Secure web gateways scan incoming internal internet traffic for malware and filter access to risky sites.

12 Top Secure Web Gateway - SWG Vendors in 2025

2

Secure Web Gateways (SWG)

What Is a Secure Web Gateway (SWG)? | Microsoft Security

CASB

Secure Web Gateway (SWG)
FWaaS

SD-WAN

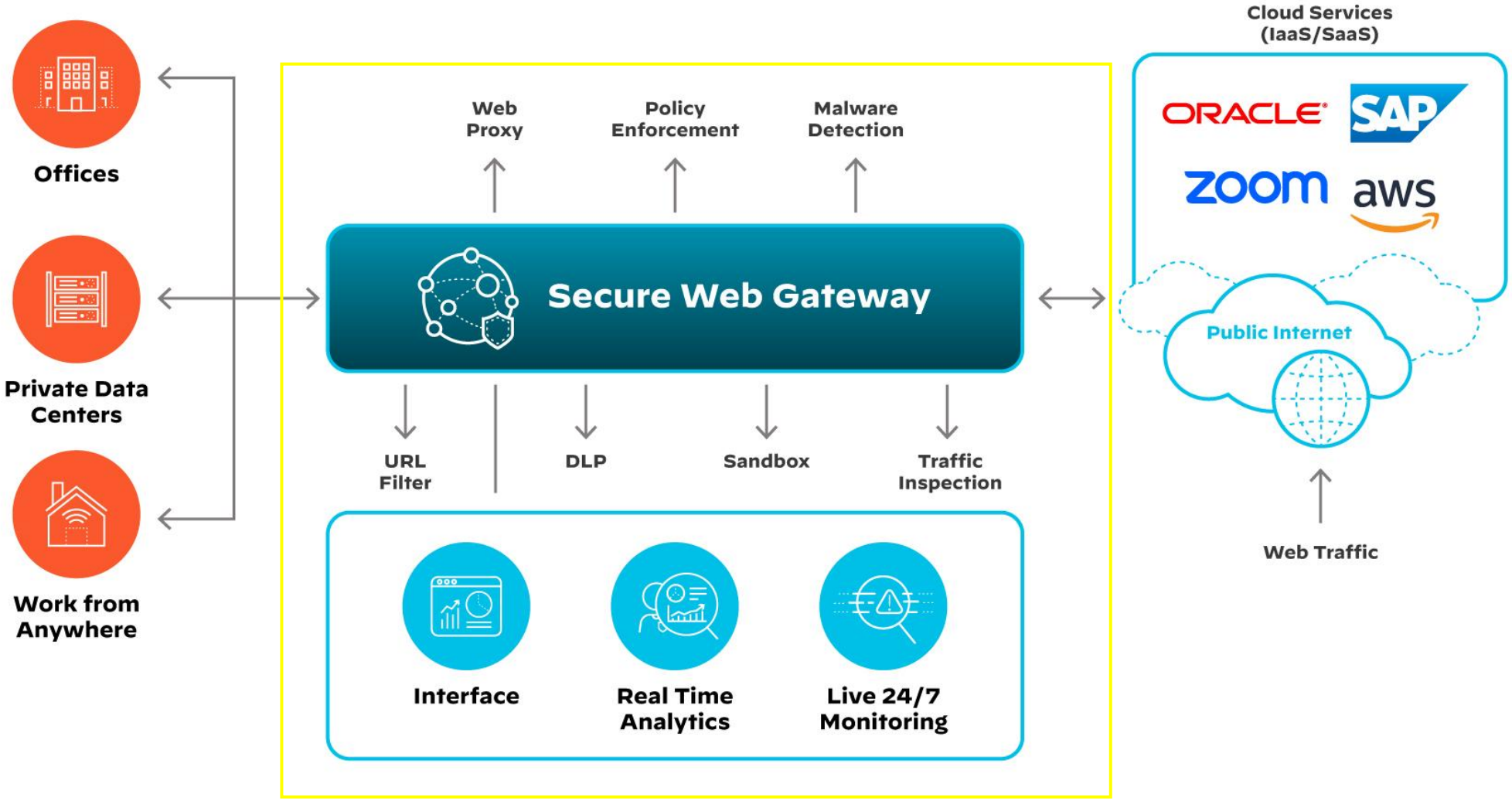
Zero Trust Network Access (ZTNA)

Why Are Secure Web Gateways Essential?

- **Threat Prevention** – Blocks malware, ransomware, and zero-day exploits via real-time URL filtering and sandboxing.
- **Data Loss Protection (DLP)** – Monitors outbound traffic to prevent sensitive data leaks.
- **Compliance Enforcement** – Ensures adherence to regulations like GDPR, HIPAA, and industry-specific mandates.
- **Remote Work Security** – Secures distributed teams with consistent policies across locations.
- **Bandwidth Optimization** – Controls non-business traffic (e.g., streaming, social media) to improve network performance.

2

Secure Web Gateway (SWG) - Capabilities

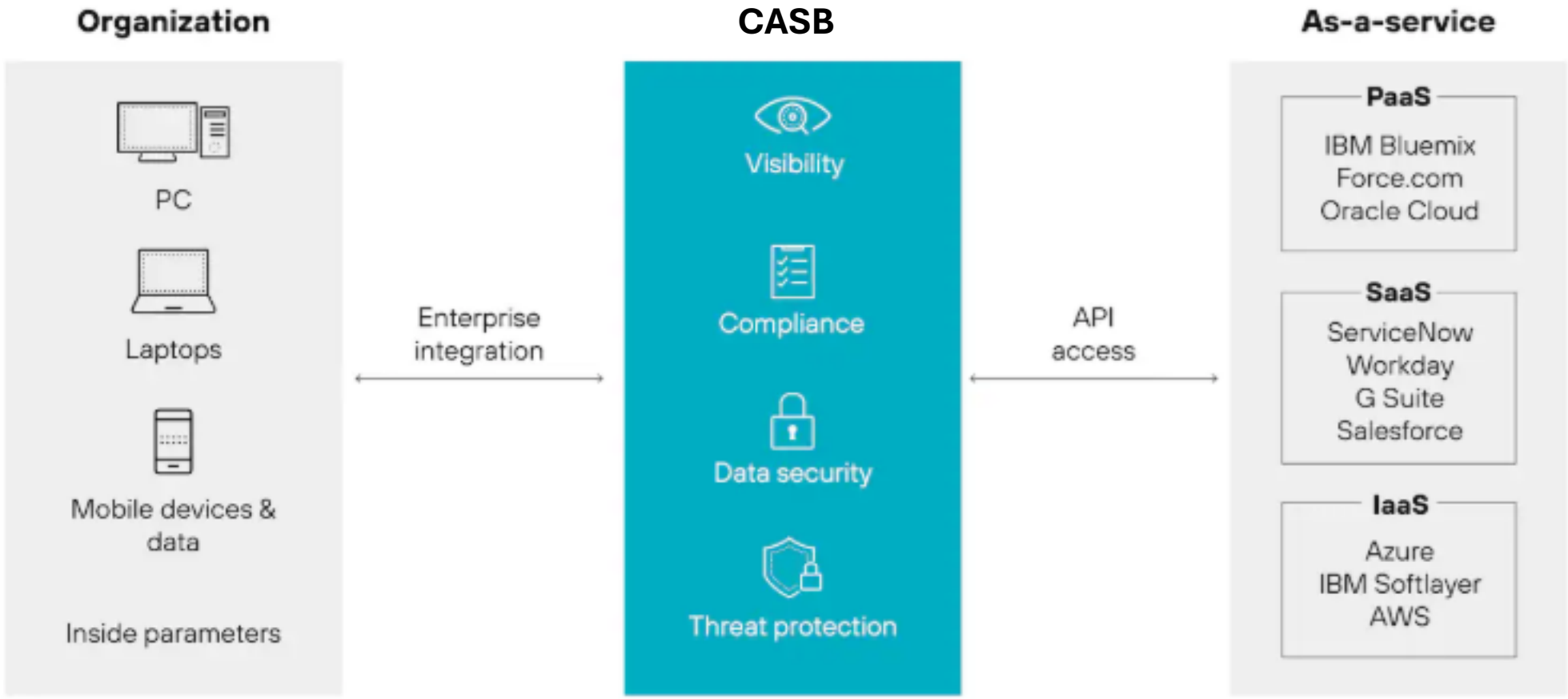


12 Top Secure Web Gateway - SWG Vendors in 2025

2

Secure Web Gateway (SWG) – Vendors as per Gartner

3 Cloud Access Security Brokers (CASB) – Security tool

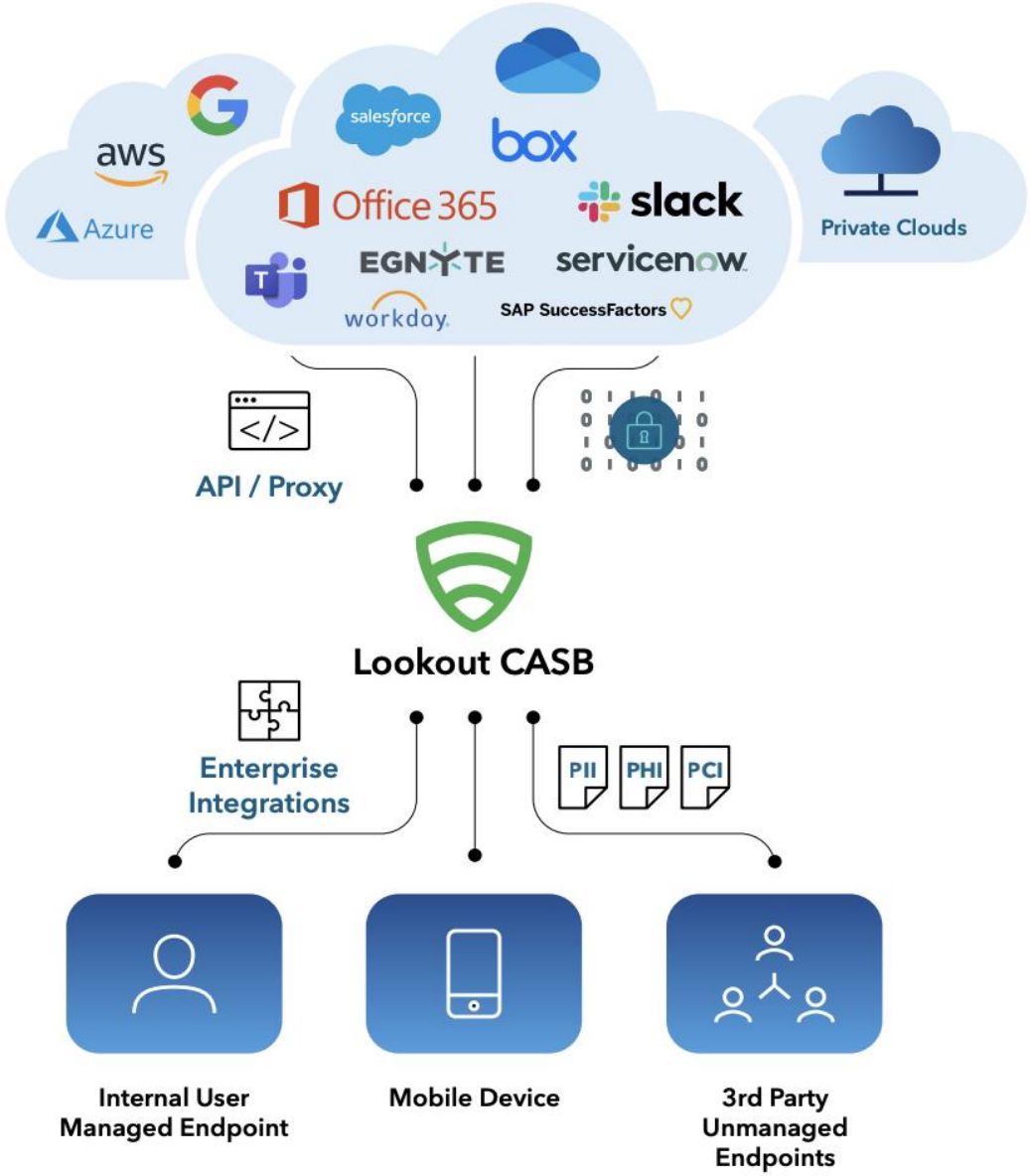


A cloud access security broker (CASB) is a security tool that acts as an intermediary between an organization's on-premises infrastructure and cloud service providers. It extends security measures to the cloud, enforcing policies and providing visibility into cloud application usage. CASBs operate across various cloud models: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). They protect organizational data by managing security functions like authentication, authorization, and encryption.

What Is a CASB (Cloud Access Security Broker)? | 101 Guide - Palo Alto Networks

3

Cloud Access Security Brokers (CASB) – Solution Capabilities



3

Cloud Access Security Brokers (CASB) – Top Vendors

The Top 10 Cloud Access Security Broker (CASB) Solutions

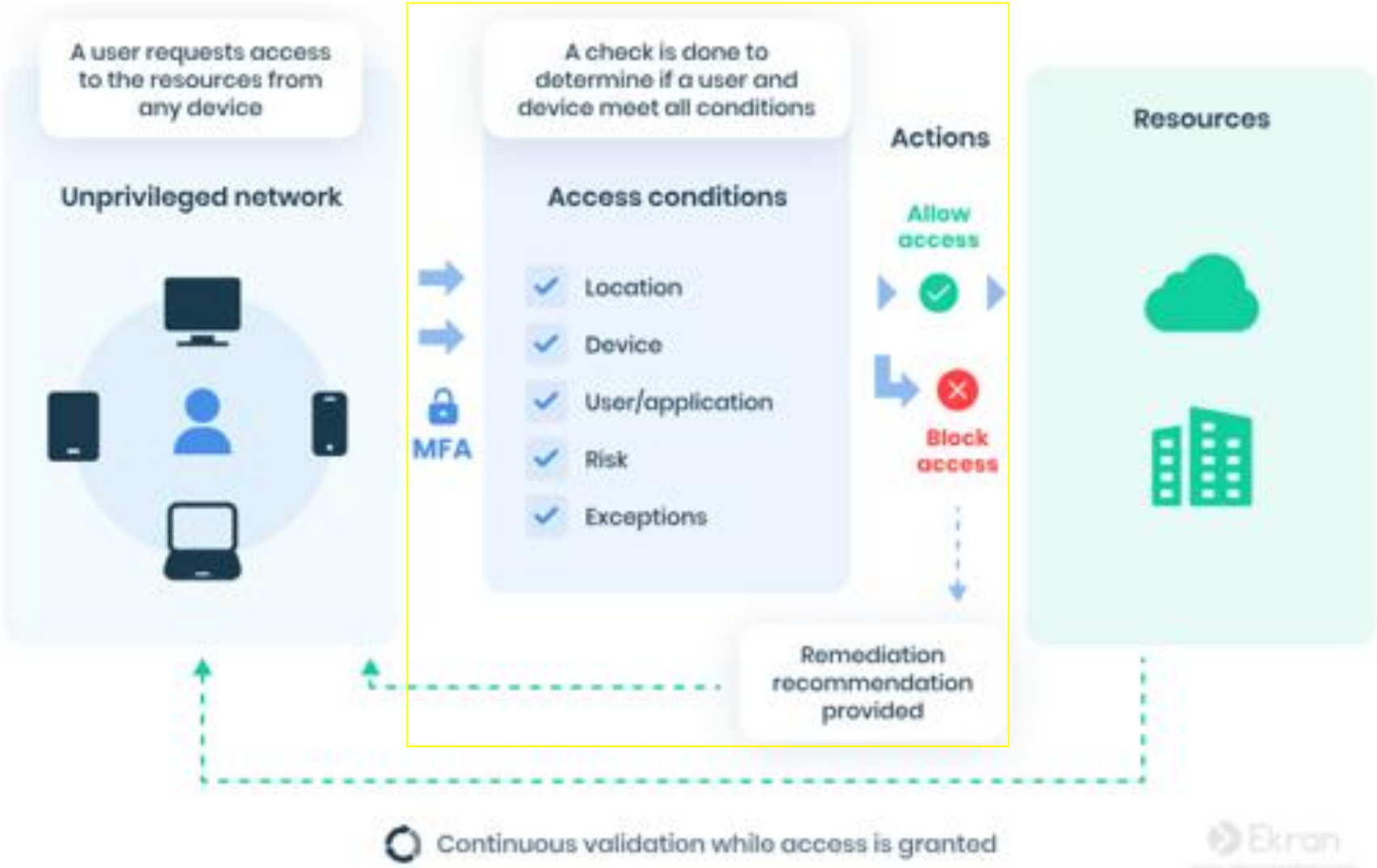
4

Zero Trust Network Access (ZTNA) – Framework

- The **Zero Trust Framework** is a modern security model designed to address the complexities of today's digital environments.
- It is not a product or service but a strategic approach to cybersecurity that emphasizes the principle of "never trust, always verify."
- **Verify Explicitly**: Always authenticate and authorize based on all available data points, such as user identity, location, device health, and service access requirements.
- **Use Least Privilege Access**: Limit access to resources using Just-In-Time (JIT) and Just-Enough-Access (JEA) principles, along with adaptive policies and data protection mechanisms.
- **Assume Breach**: Minimize the impact of potential breaches by segmenting access, enforcing end-to-end encryption, and leveraging analytics for threat detection and response.
- **Implementing Zero Trust** requires a tailored approach based on an organization's existing infrastructure, security maturity, and specific needs. It involves integrating Zero Trust principles across the entire organization, from identity management to network segmentation and application security. Tools like **Microsoft Entra ID** and Azure services can help organizations align with Zero Trust strategies.

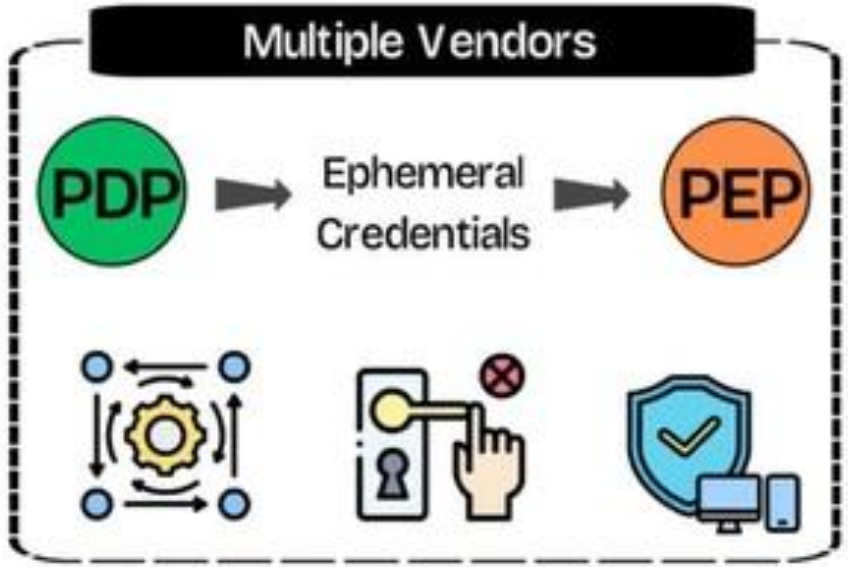
4

Zero Trust Network Access (ZTNA) – Conditions & Actions



Zero Trust Network Access (ZTNA) – Decision / Enforcement

- Software Defined Perimeter (SDP)
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)



4

Zero Trust Network Access (ZTNA) – Decision / Enforcement / Vendors

SASE

- zScaler Policy Engine
- Cloudfare One
- FortiSASE Controller

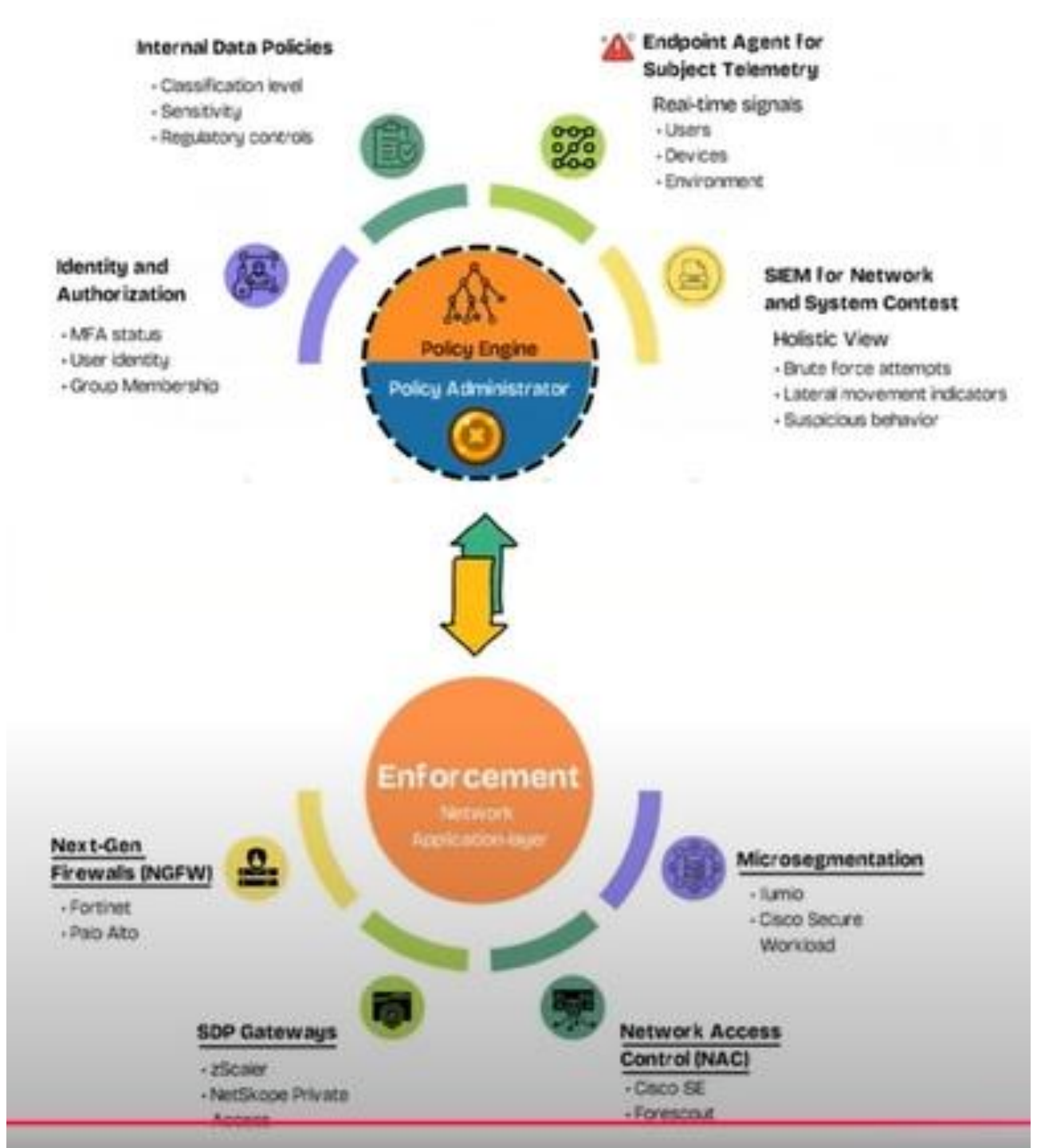
Decision

Most Critical Component in ZTA

ZTA

- StrongDM
- Appgate SDP
- BeyondCorp

1. Dynamic Evaluation of Multiple Datapoints
2. Continuous Input Assessment
3. Ephemeral Base Authorization
4. Integration with Enforcement Point



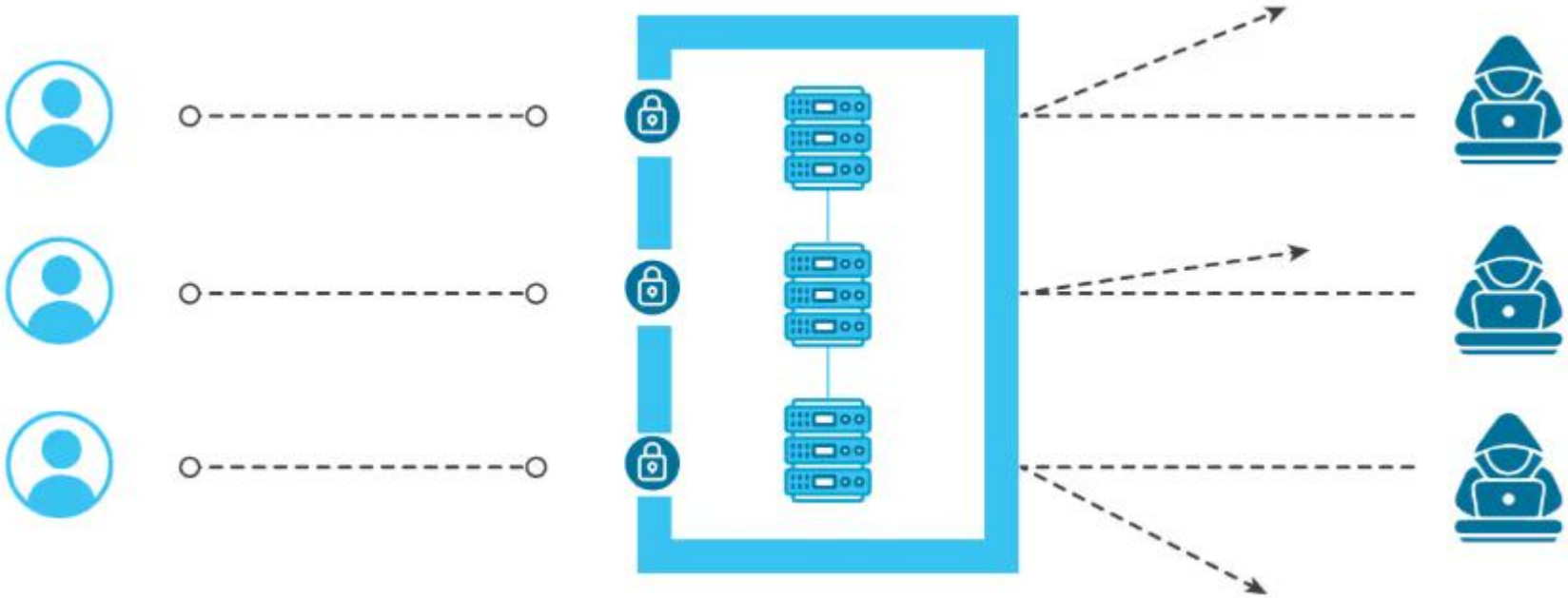
5

Firewall Wall as a Service (FWaaS) – Blocks the latest cyber threats in the cloud

- A cloud firewall is a security product that, like a traditional firewall, filters out potentially malicious network traffic.
- Unlike traditional firewalls, cloud firewalls are hosted in the cloud. This cloud-delivered model for firewalls is also called firewall-as-a-service (FWaaS).
- Cloud-based firewalls form a virtual barrier around cloud platforms, infrastructure, and applications, just as traditional firewalls form a barrier around an organization's internal network.
- Cloud firewalls can also protect on-premise infrastructure.

5

Firewall Wall as a Service (FWaaS) – Blocks the latest cyber threats in the cloud



Cisco
Advanced protection

Palo Alto Networks
AWS integration

Fortinet
Comprehensive package

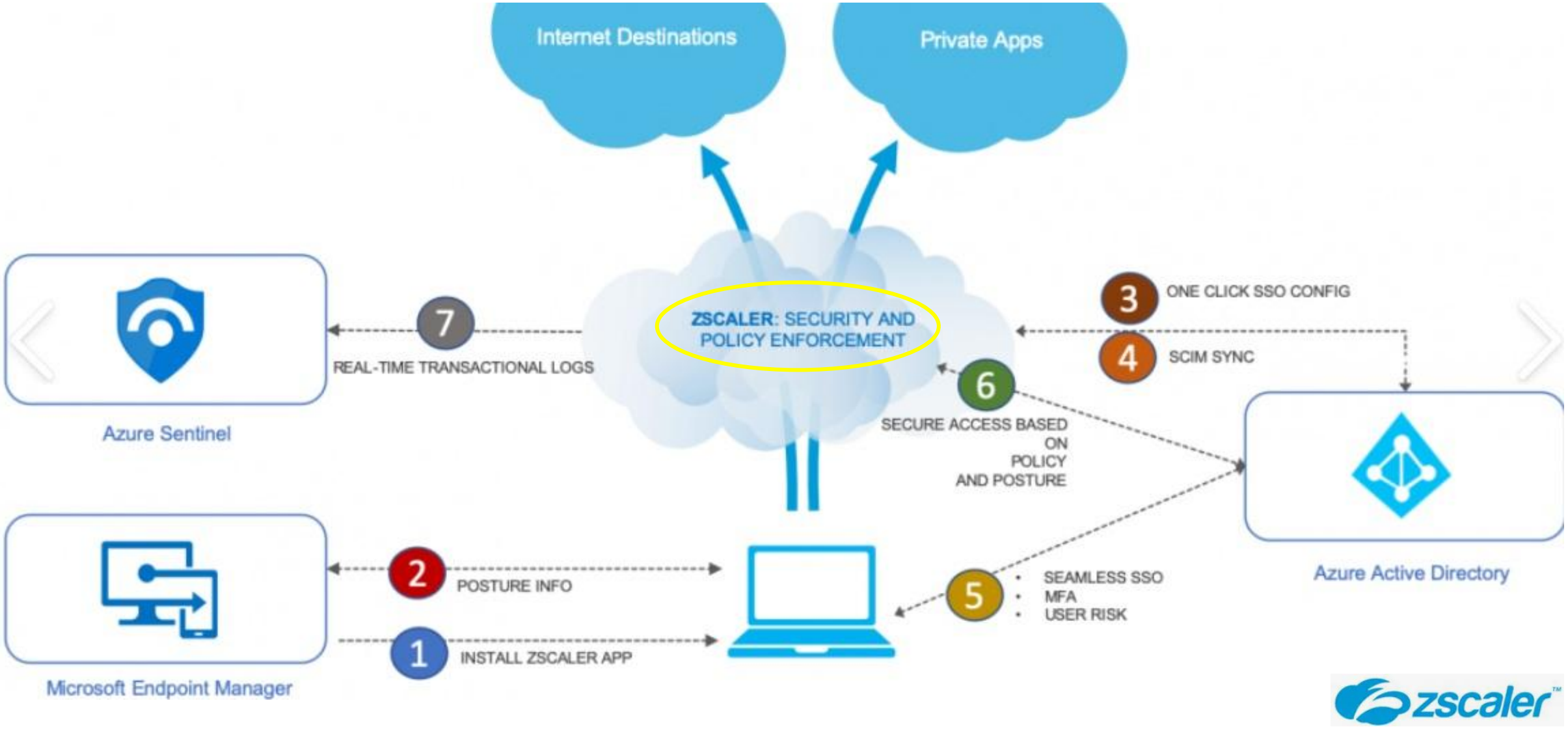
Zscaler
Virtual office security

Cato Networks
Advanced inspection

Check Point
Next-gen technology

5

Firewall Wall as a Service (FWaaS) – Zscaler Policy Enforcement



Cloud platform adoption plans

Every business has different needs and will therefore follow a slightly different process for cloud migrations. Cloud providers can help businesses set up their migration process. Most cloud migrations will include these basic steps:

1. **Establish goals**: What performance gains does a business hope to see? On what date will legacy infrastructure be deprecated? Establishing goals to measure against helps a business determine if the migration was successful or not.

2. **Create a security strategy**: Cloud cybersecurity requires a different approach compared to on-premise security. In the cloud, corporate assets are no longer behind a firewall, and the network perimeter essentially does not exist. Deploying a cloud firewall or a web application firewall may be necessary.

3. **Copy over data**: Select a cloud provider and replicate existing databases. This should be done continually throughout the migration process so that the cloud database remains up-to-date.

4. **Move business intelligence**: This could involve refactoring or rewriting code (see below). It can be done piecemeal or all at once.

5. **Switch production from on-premise to cloud**: The cloud goes live. The migration is complete.

7

Cloud Security Initiatives 2025

- **Identity Hardening**: Prioritize identity hardening across cloud and hybrid environments, enforcing multi-factor authentication, and removing legacy trust paths to adopt zero-trust principles.

- **Visibility and Visibility Gaps**: Address visibility gaps and ensure that security teams can see what attackers see, using tools like CSPM and ASM.

- **Unified Platforms**: 97% of respondents prefer unified cloud security platforms with centralized dashboards to simplify policy configuration and enhance visibility across an organization's cloud footprint.

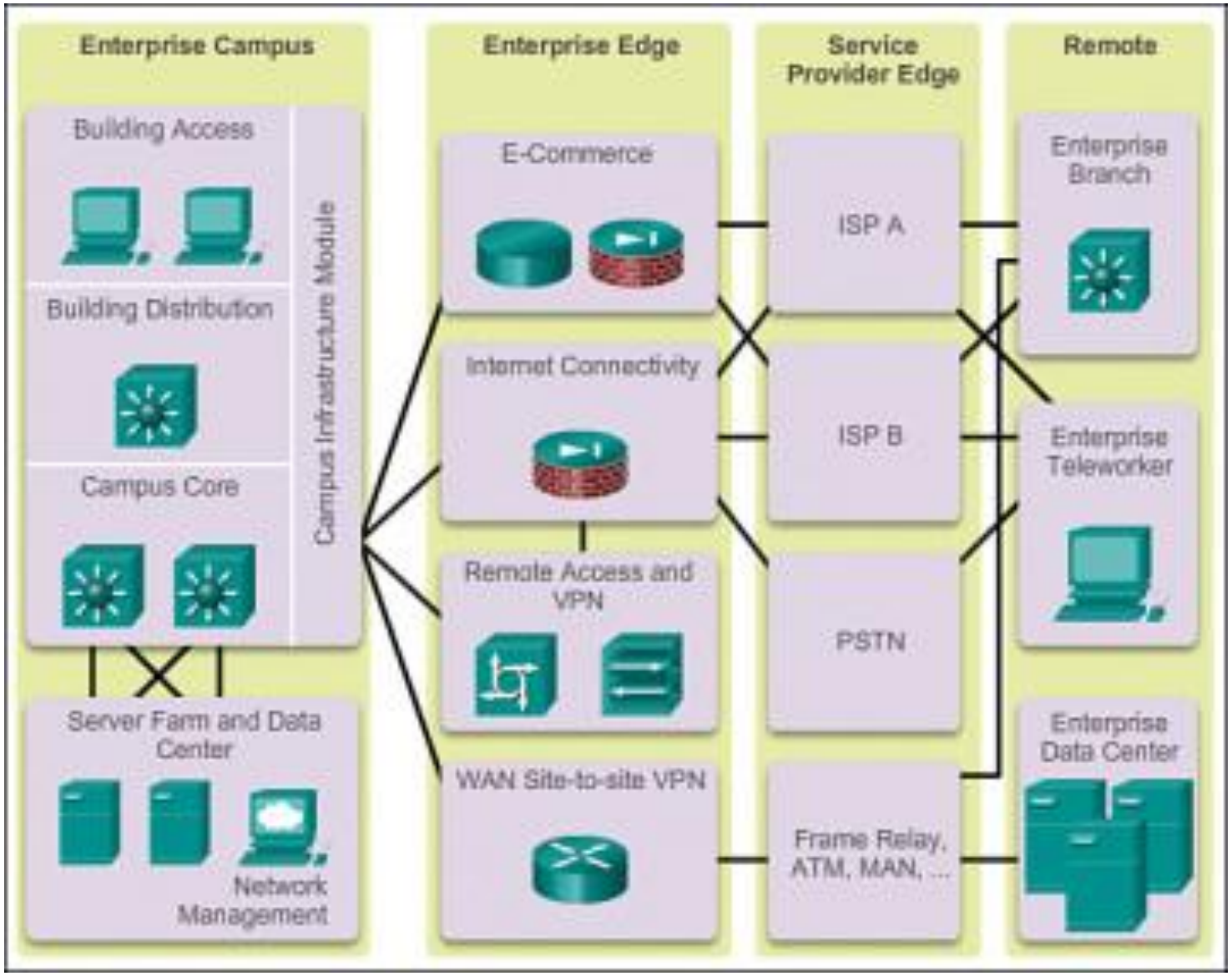
- **AI Automation**: Automate repetitive tasks with AI to manage security at scale, addressing complex environments with fewer resources and reducing the risk of human error.

- **Zero-Trust Principles**: Adopt zero-trust principles to protect against identity pivots and ensure that security measures are consistent across all cloud environments.

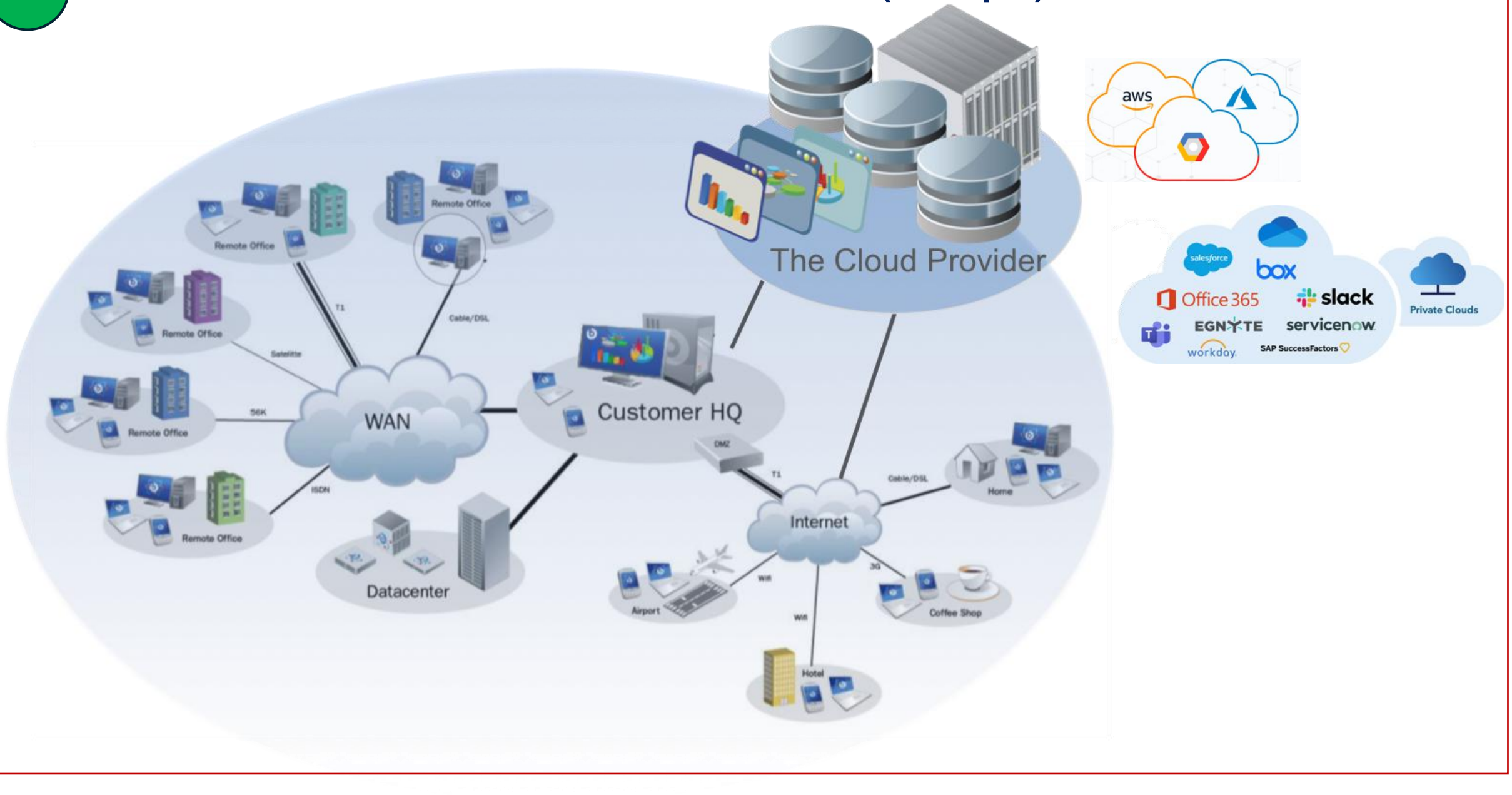
- **Ransomware and Extortion**: Be prepared for ransomware and multifaceted extortion as the most disruptive forms of cyber crime, impacting various sectors and countries.

Organizations should review their current security processes to identify repetitive or resource-intensive tasks that could be automated with AI and prepare for the evolving cloud landscape.

Network Architecture – Current State (example)

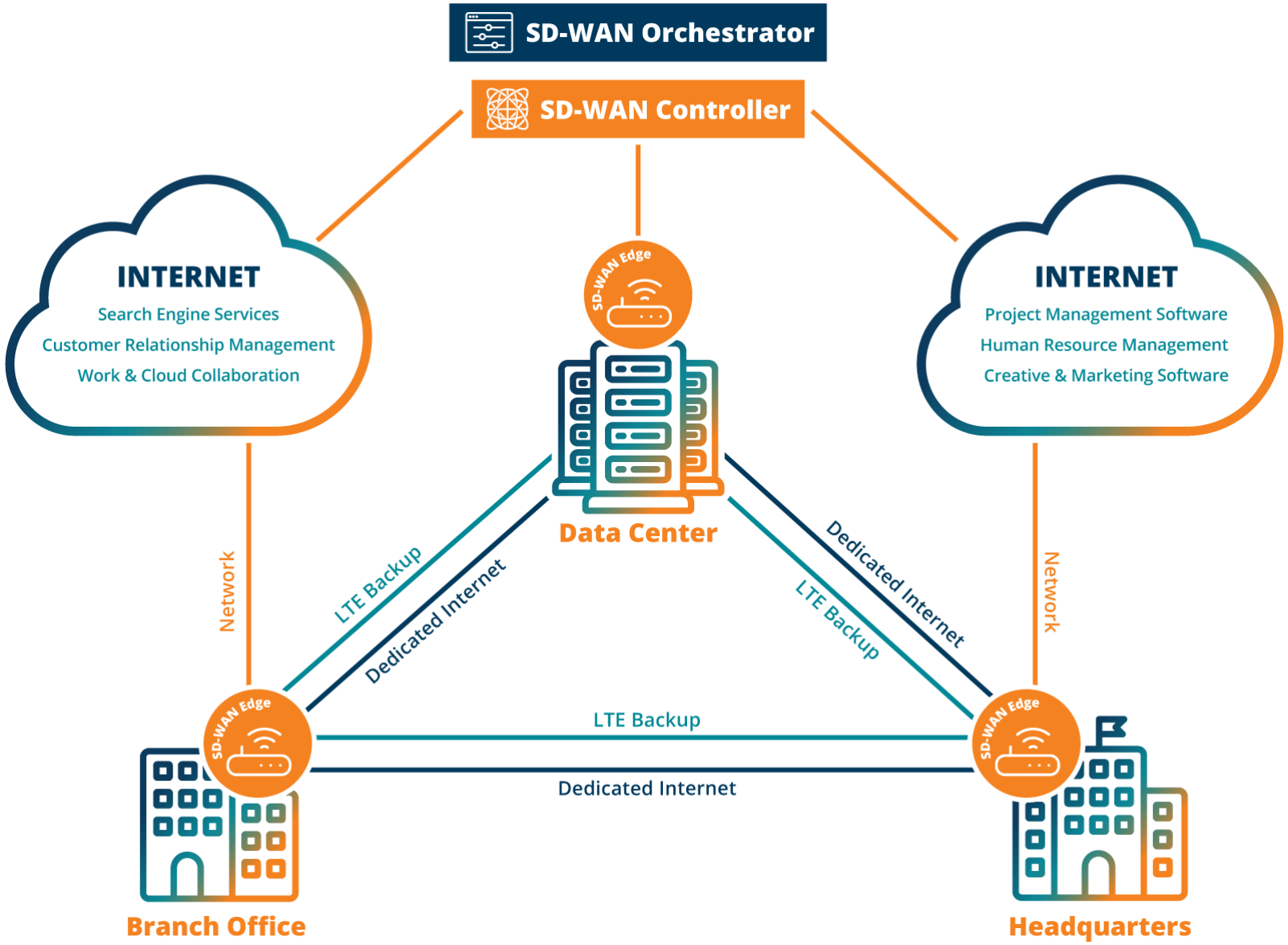


Network Architecture – Transition/Future State (example)

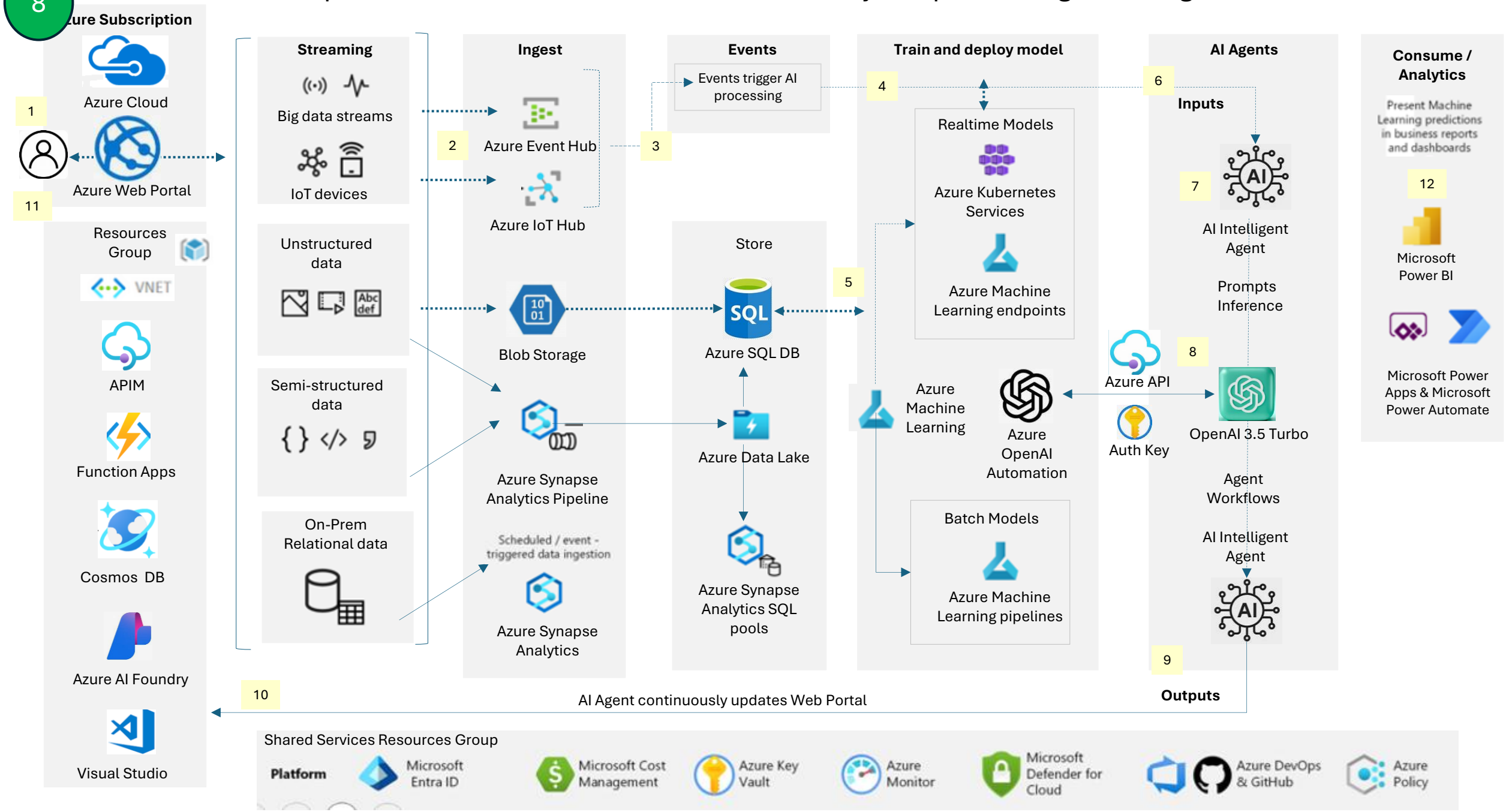


8

Network Architecture – Transition/Future State w/ SD-WAN



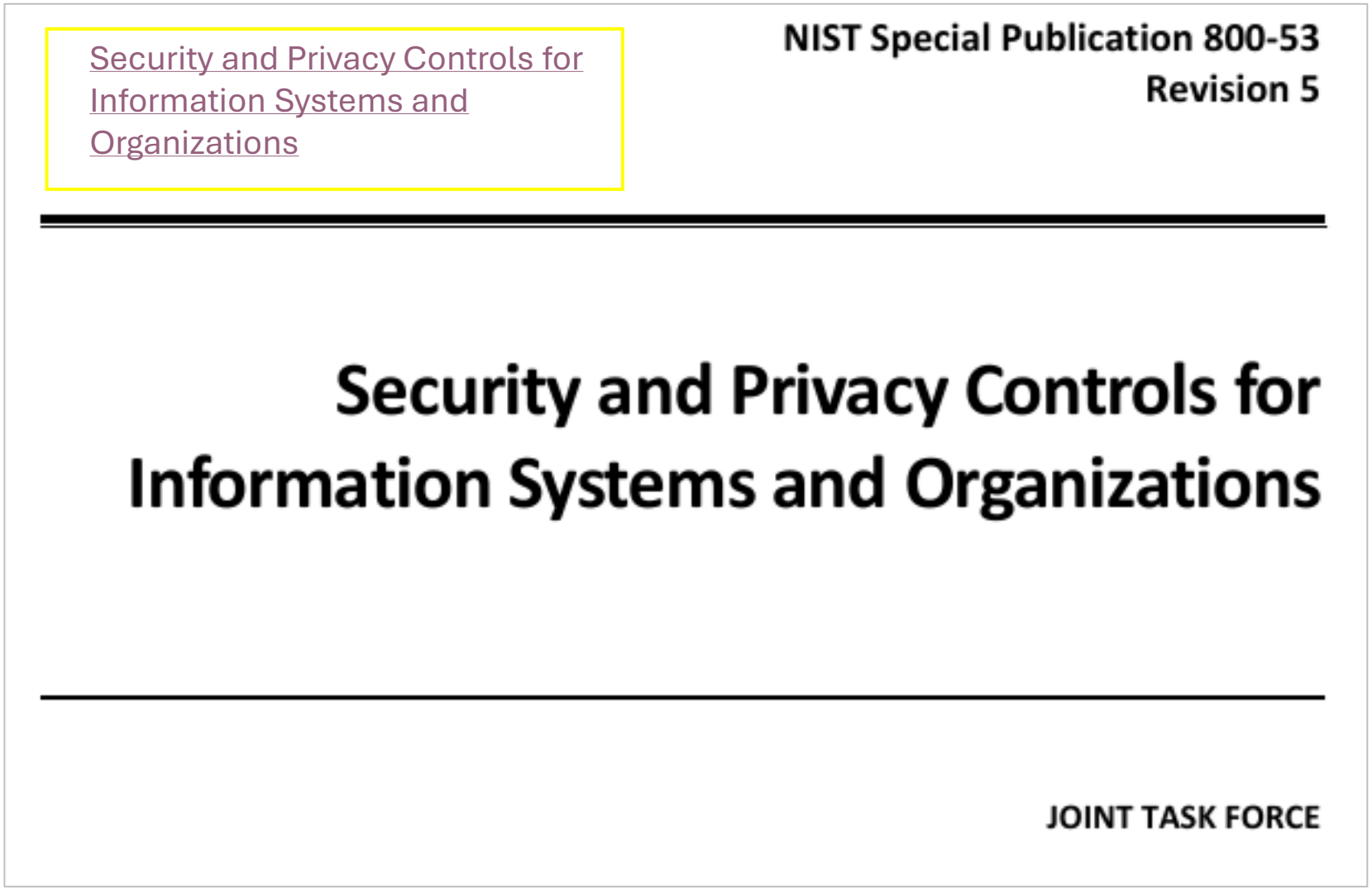
8 Azure Cloud Example - Draft v2: Azure Web Portal -> AI Foundry -> OpenAI AI Agents Integration / Workflows



9

Security incident containment / remediation – NIST 800-53

Security and Privacy Controls for Information Systems and Organizations



9

Security incident containment / remediation – SIEM vendors

Security Information and Event Management Market Size, Share & Growth Report, 2030

Security incident containment / remediation – Ransomware – NIST procedures

NIST's National Cybersecurity Center of Excellence (NCCoE) has published Practice Guides to demonstrate how organizations can develop and implement security controls to combat the data integrity challenges posed by ransomware and other destructive events.

These are described in:

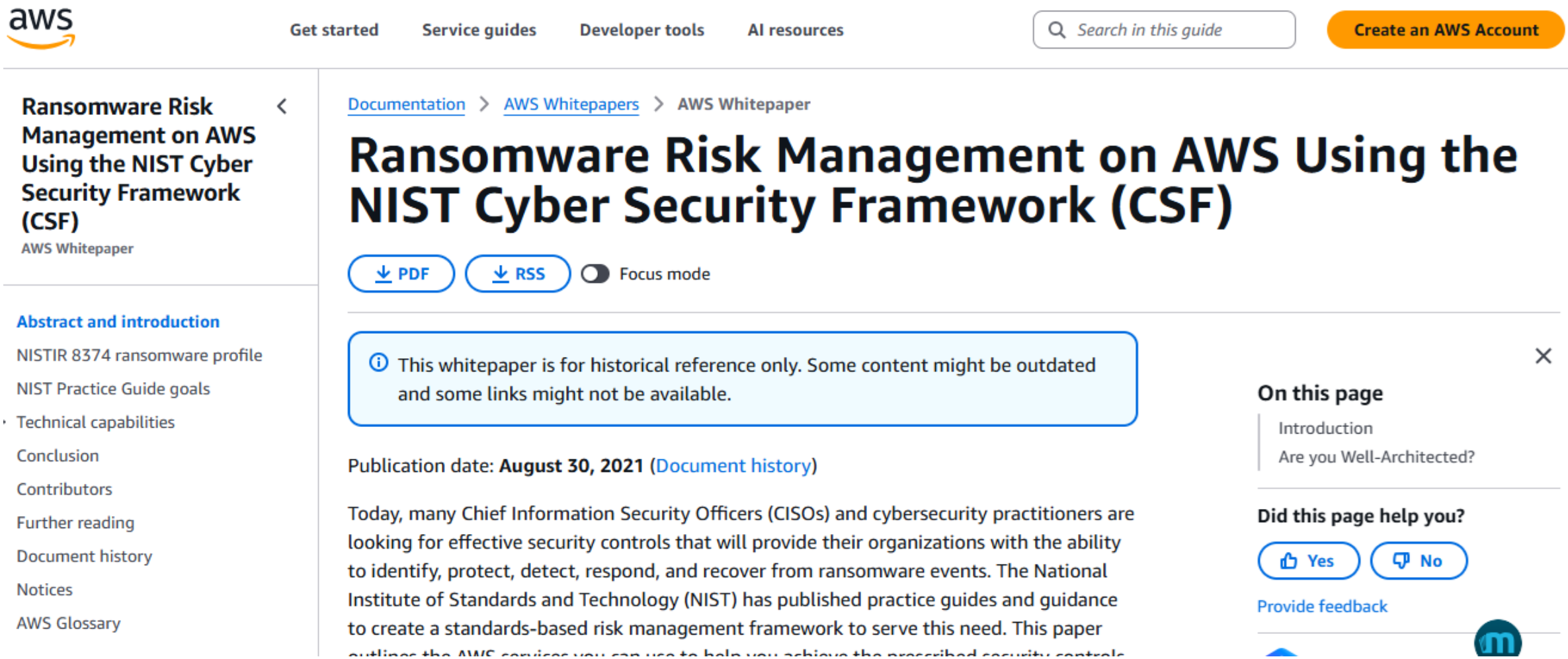
- NIST Special Publication (SP) 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events
- SP 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events,
- SP 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

In addition, the draft NISTIR 8374, Cybersecurity Framework Profile for Ransomware Risk Management, provides guidance on how to defend against the threat, what to do in the event of an event, and how to recover from it. This framework can be used by organizations to improve their risk posture. It can also help organizations seeking to implement a risk management framework that deals with ransomware threats.

9 Security incident containment / remediation – Microsoft procedures

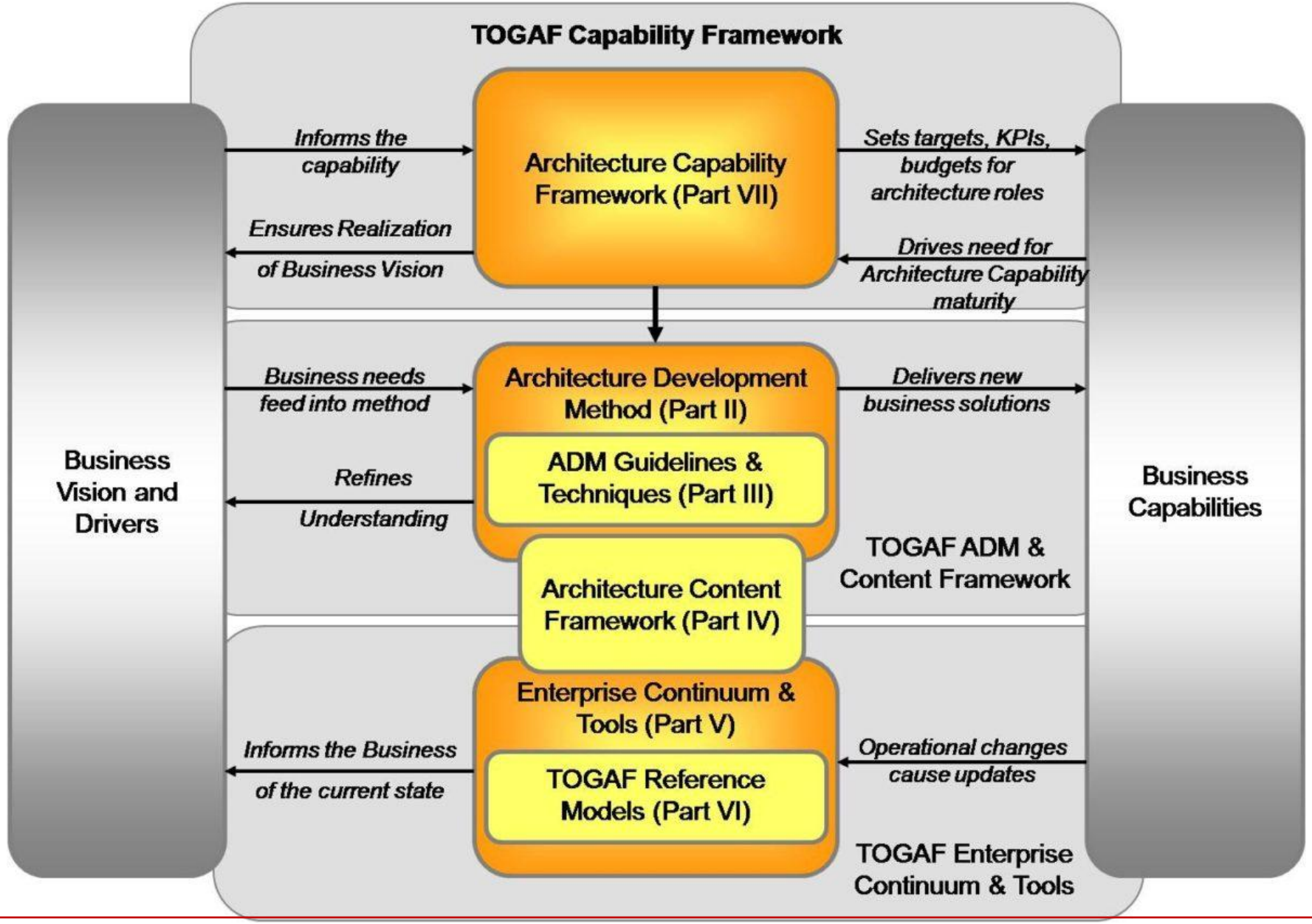
Microsoft security incident management: Containment, eradication, and recovery - Microsoft Service Assurance | Microsoft Learn

9 Security incident containment / remediation – Ransomware - NIST procedures

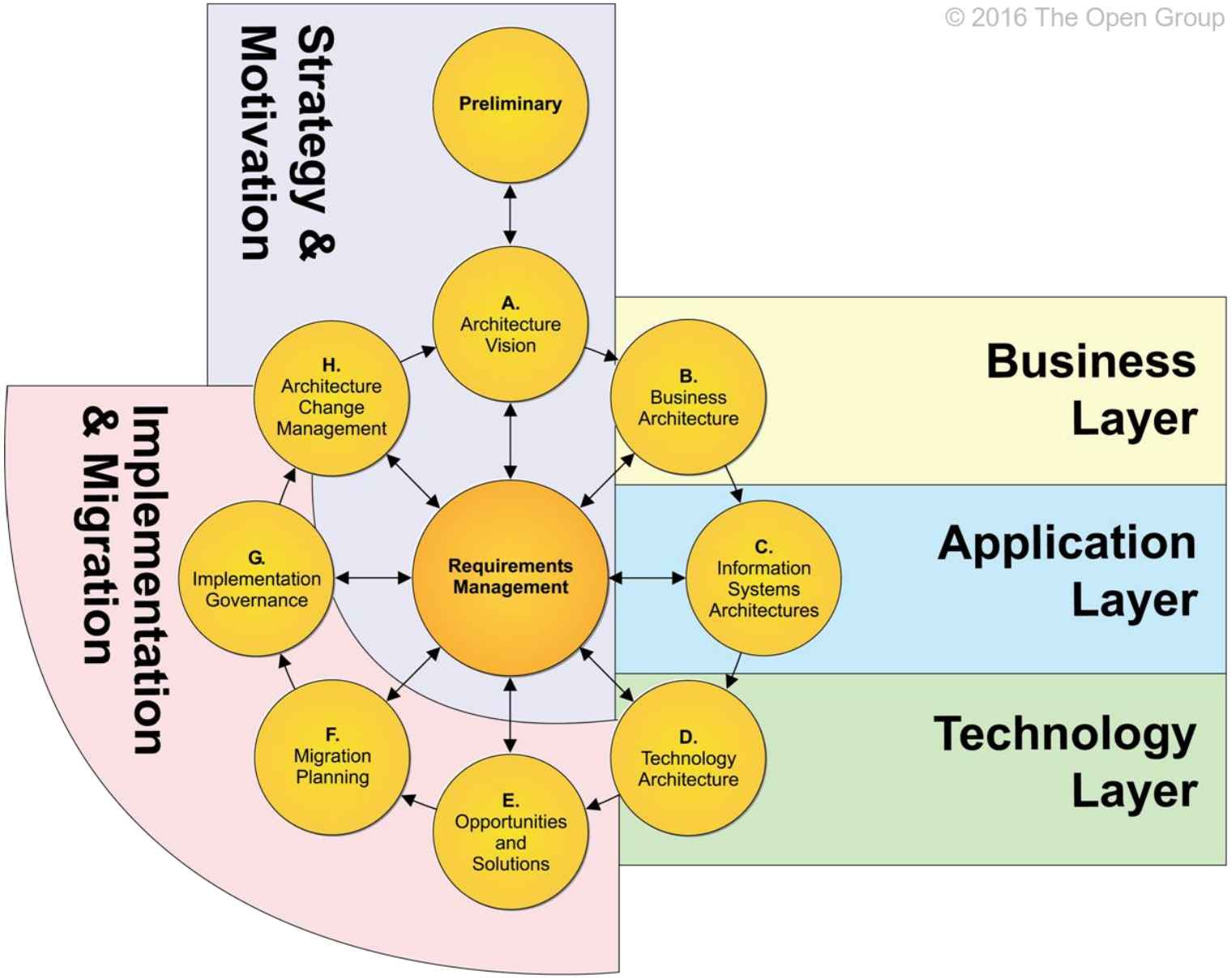


[Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF) - Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)]

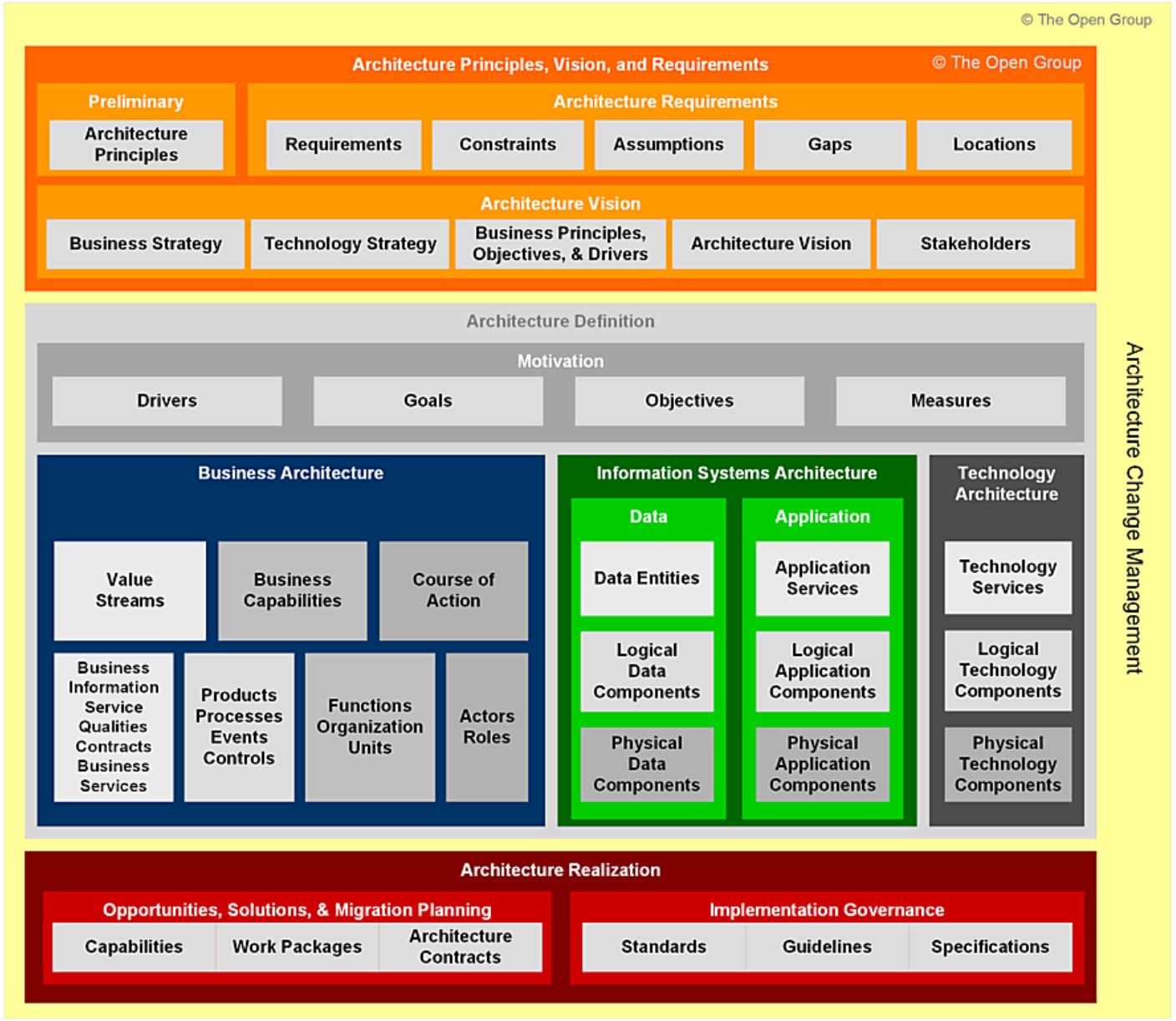
The Open Group Architecture Project (TOGAF) – Enterprise Architecture Framework



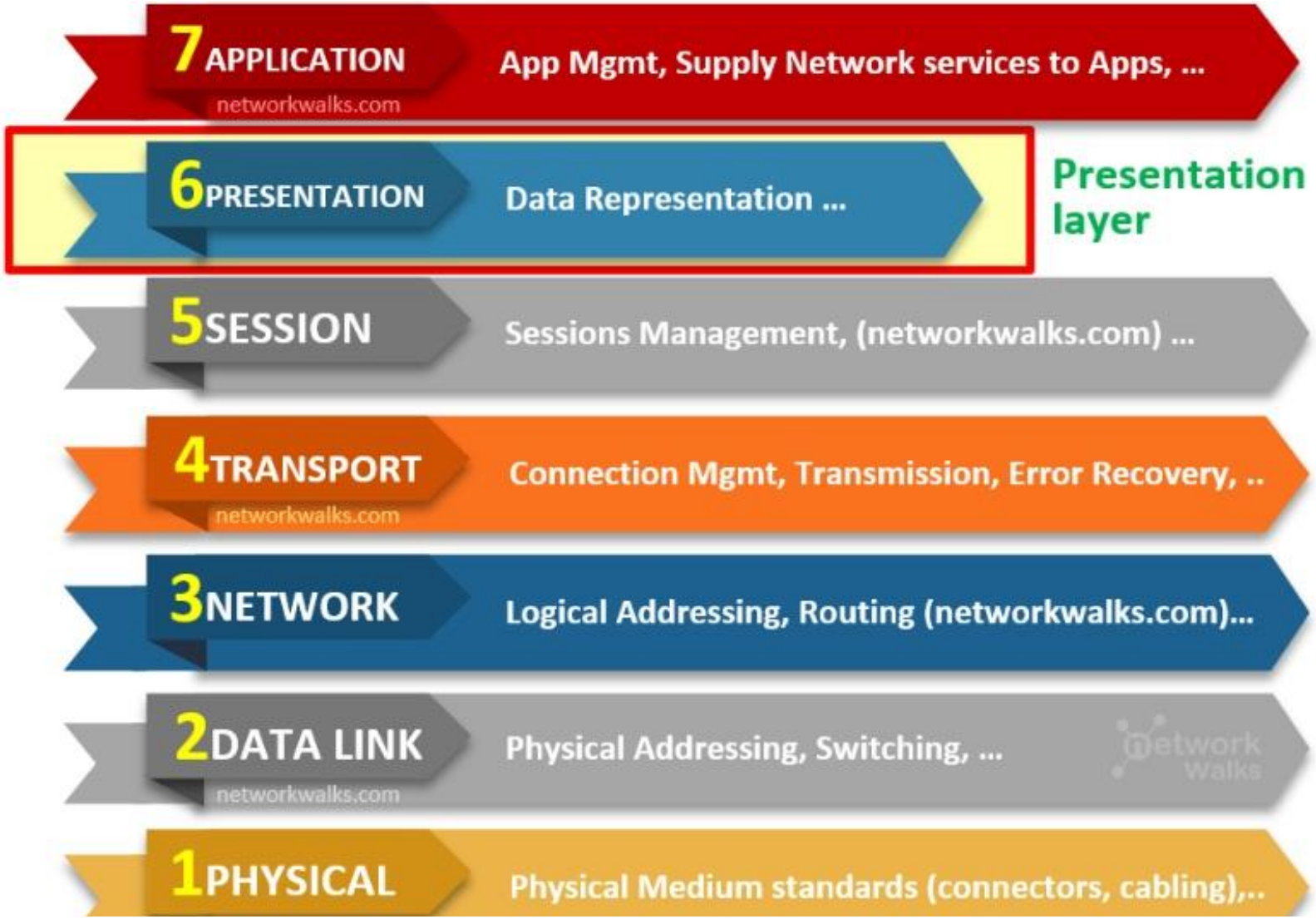
The Open Group Architecture Project (TOGAF) – Enterprise Architecture Framework



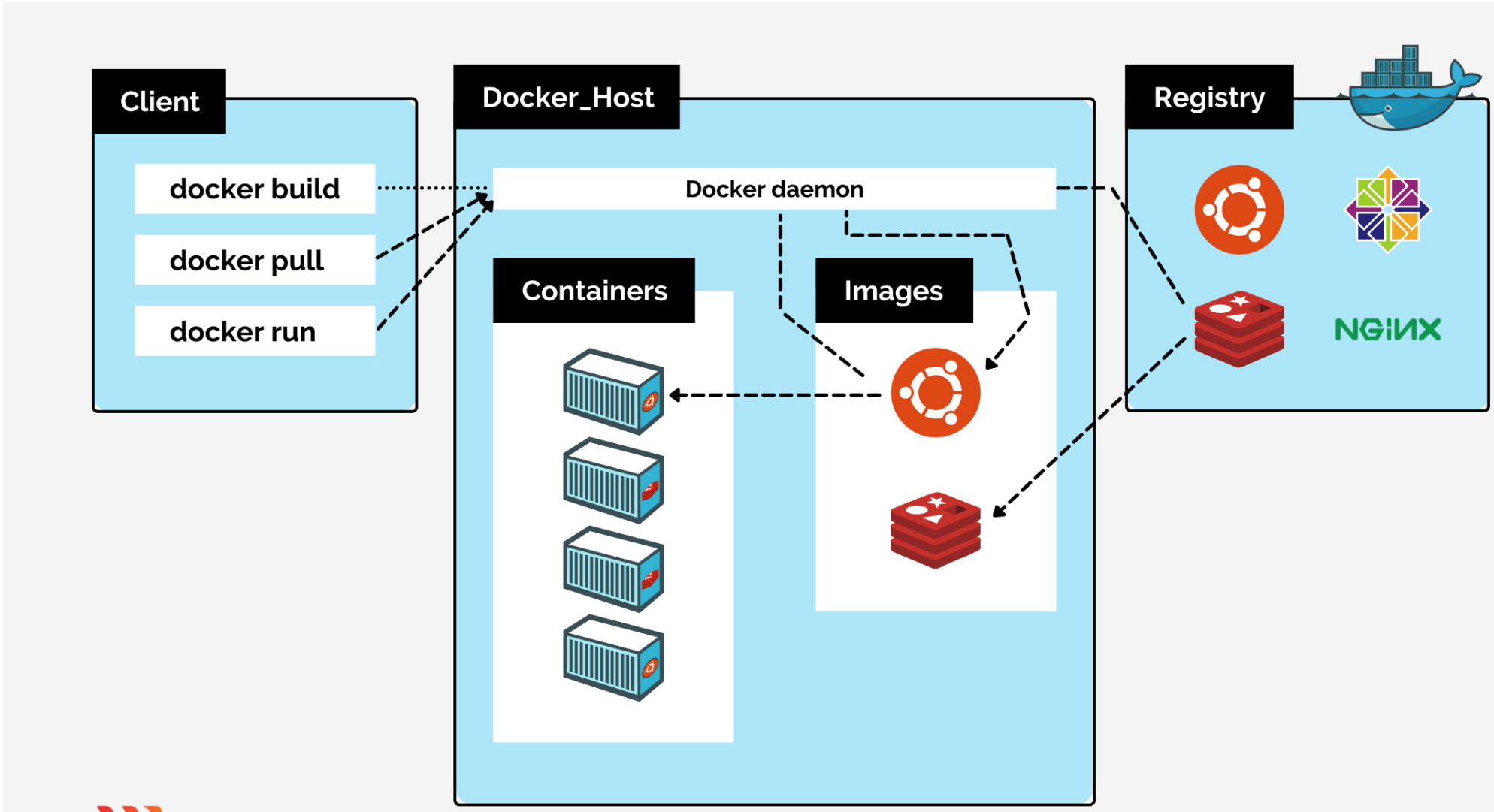
The Open Group Architecture Project (TOGAF) – Enterprise Architecture Framework



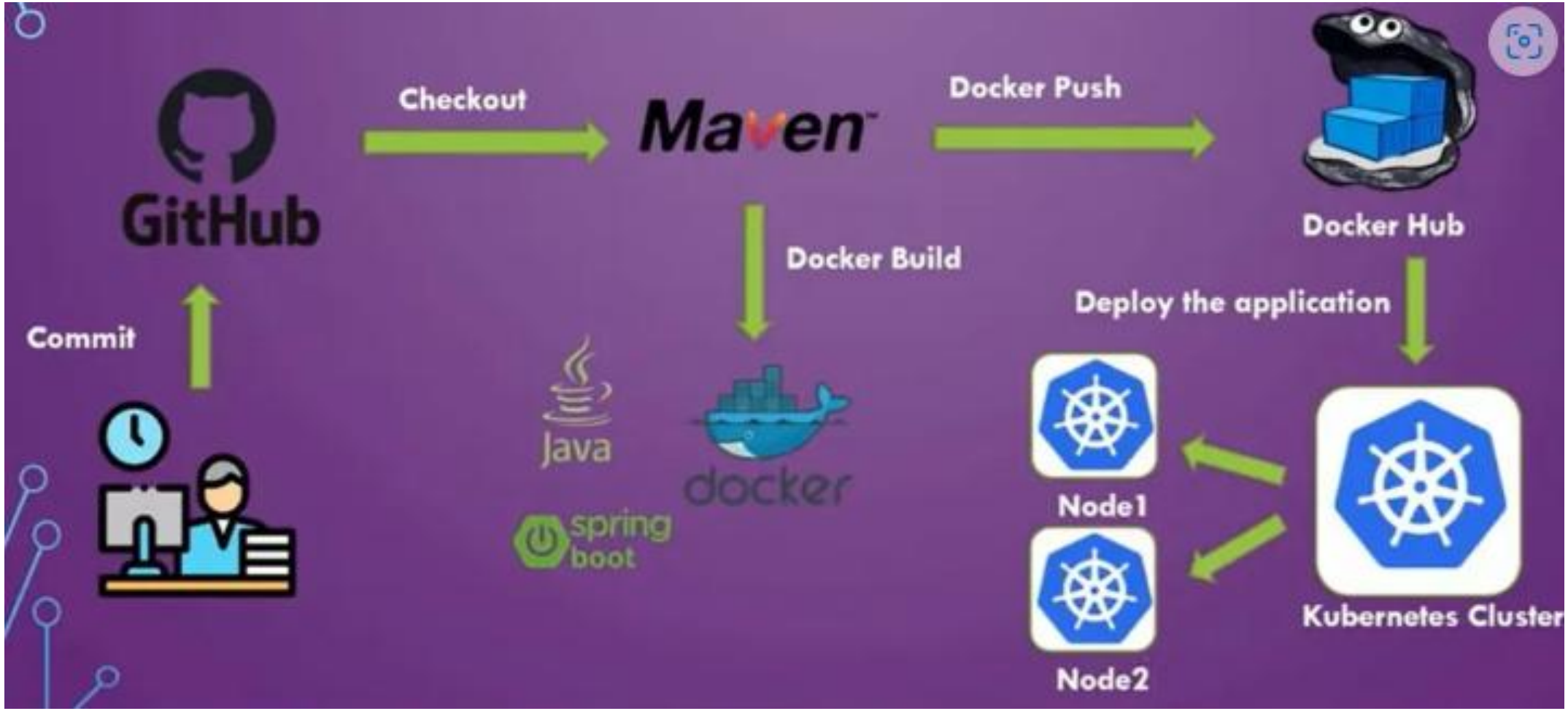
Open Systems Interconnection (OSI) model



Docker Containers



Docker Containers – Developer flow



11

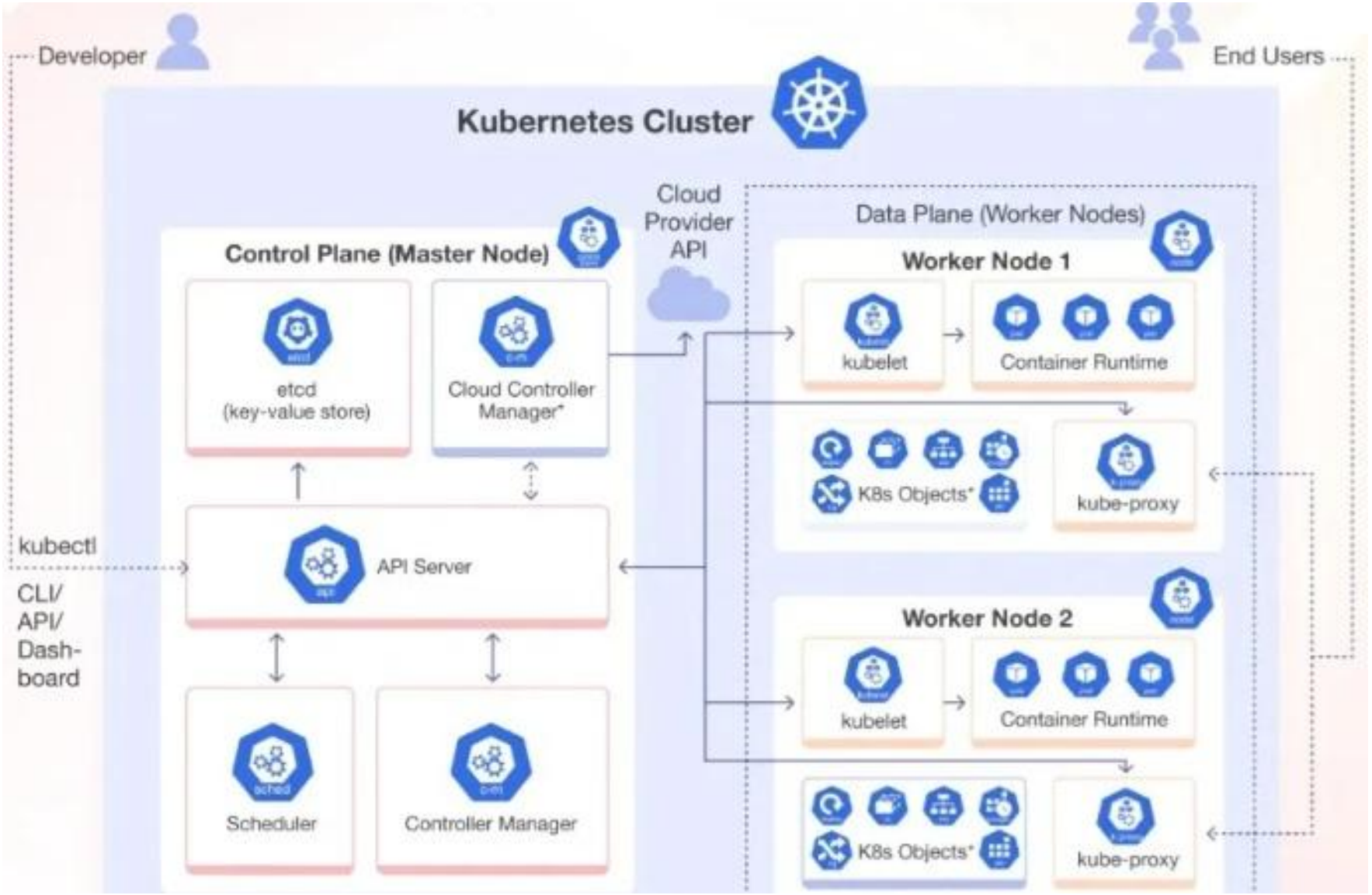
OWASP Docker Security Checklist / Links

1. Keep Host and Docker up to date
2. Do not expose the Docker daemon socket (even to the containers)
3. Set a user
4. Limit capabilities (Grant only specific capabilities, needed by a container)
5. Add –no-new-privileges flag
6. Disable inter-container communication (–icc=false)
7. Use Linux Security Module (seccomp, AppArmor, or SELinux)
8. Limit resources (memory, CPU, file descriptors, processes, restarts)
9. Set filesystem and volumes to read-only
10. Use static analysis tools
11. Set the logging level to at least INFO
12. Lint the Dockerfile at build time

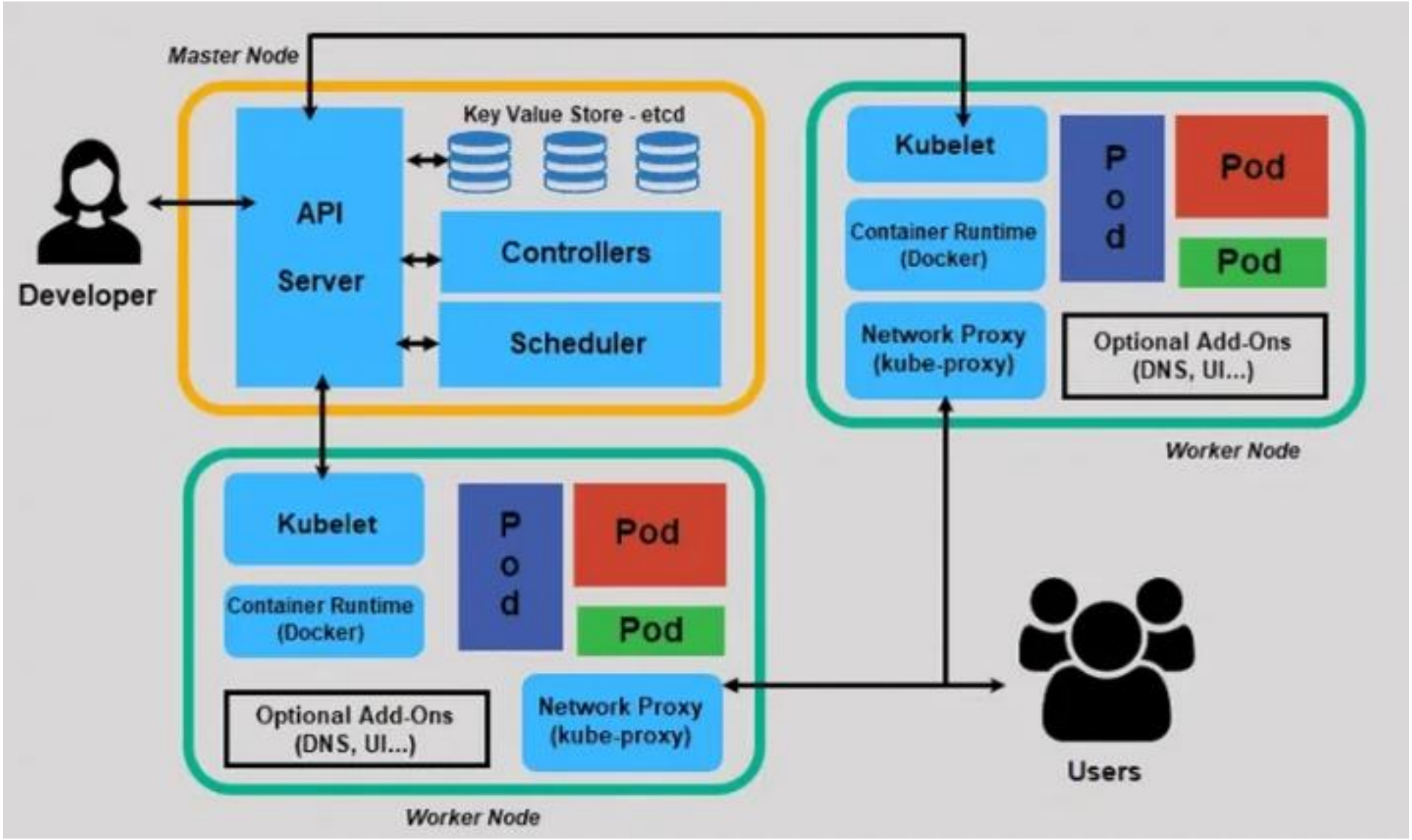
Source: Docker Security - OWASP Cheat Sheet Series

11

Kubernetes Security Cluster



Kubernetes Security Cluster – Developer flow



11

Kubernetes Security Checklist / Links

What's next

Learn about related Kubernetes security topics:

- Securing your cluster
- Known vulnerabilities in Kubernetes (and links to further information)
- Data encryption in transit for the control plane
- Data encryption at rest
- Controlling Access to the Kubernetes API
- Network policies for Pods
- Secrets in Kubernetes
- Pod security standards
- RuntimeClasses

Learn the context:

- Cloud Native Security and Kubernetes

Security | Kubernetes

Kubernetes Security - OWASP Cheat Sheet Series


Thank
You