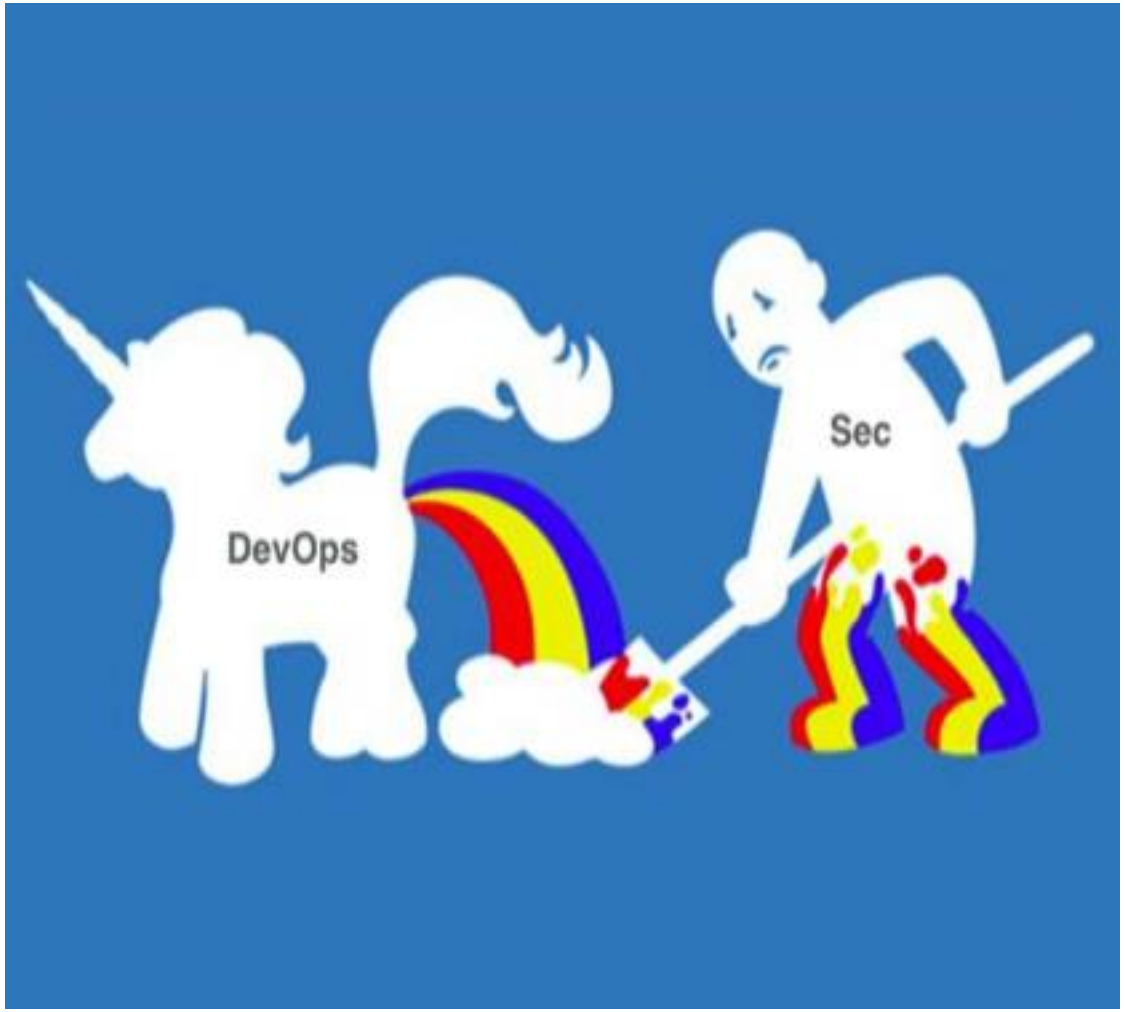
Securing and Protecting DevSecOps with Cloud-Enabled Technologies

Lisa Lorenzin, Director Transformation Strategy, Zscaler

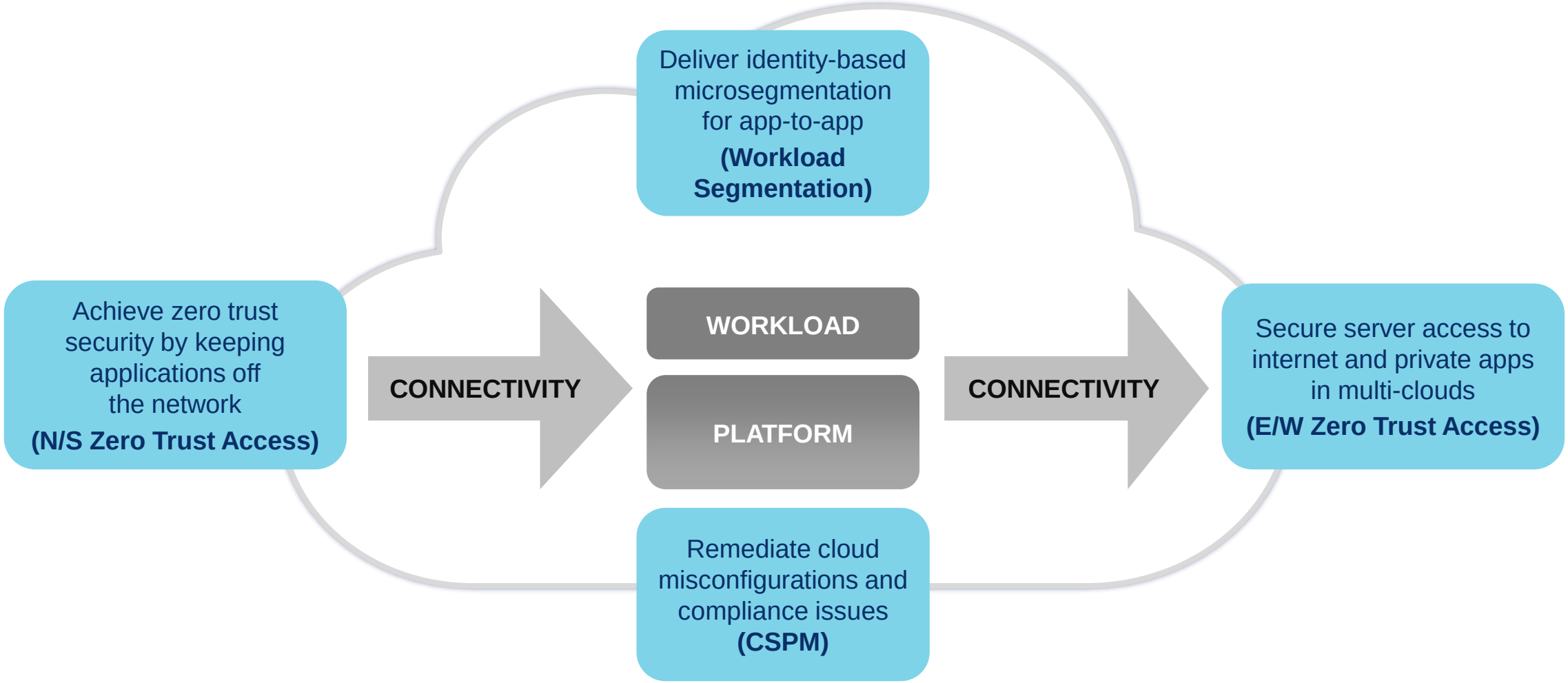
lisa@zscaler.com

Is this the current state of your DevOps and security practices?



Leveraging the cloud for DevSecOps

Cloud-Enabled DevSecOps



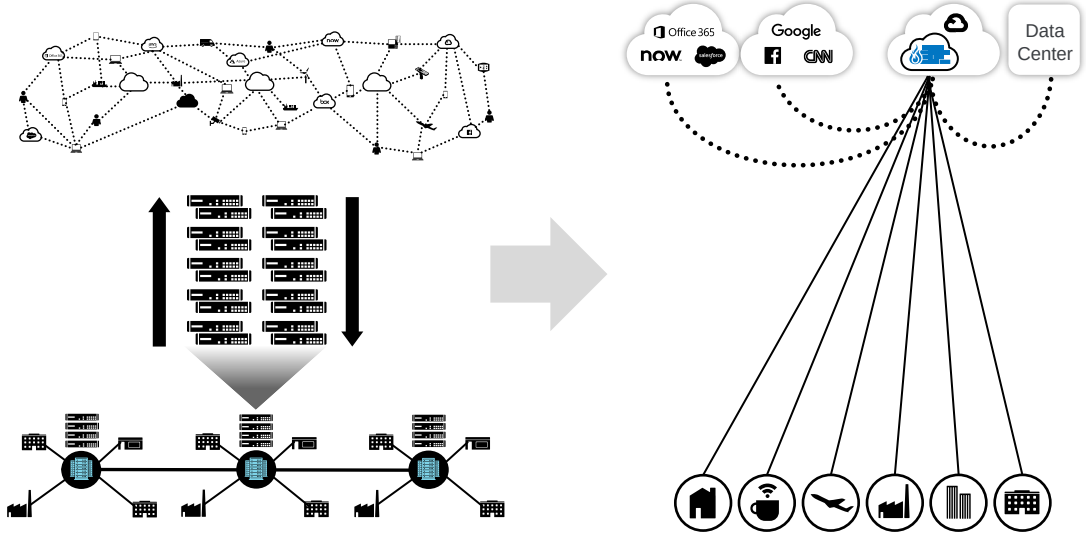
- Use zero trust security to stop exposing applications to the network
- Leverage user identity instead of the network to segment and protect applications
- Apply continuous cloud security posture management to avoid misconfigurations

Simplify DevSecOps by keeping apps off the network

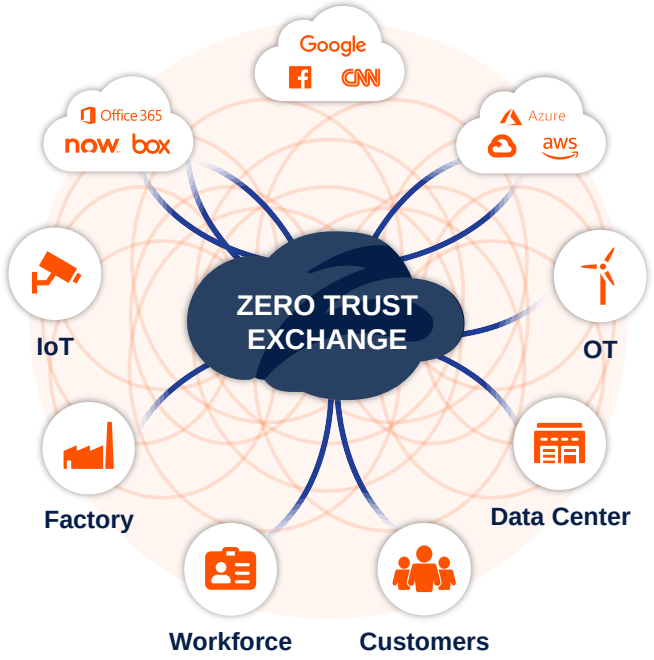
Legacy Network and Security Architectures

On-Prem Appliances

Virtual Appliances in Public Cloud



Cloud-Delivered Zero Trust Architecture



Any-to-Any connectivity: User to Apps, App to App, M2M
Any network, Any location

You control and secure your network

Castle-and-moat security creates a perimeter

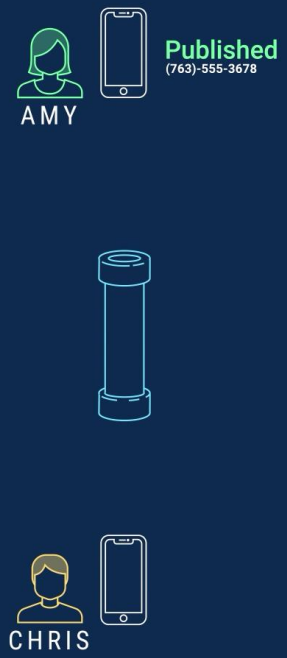
Two Opposing Approaches

Internet is the new network; it can't be secured

Securely connect users and apps using business policies

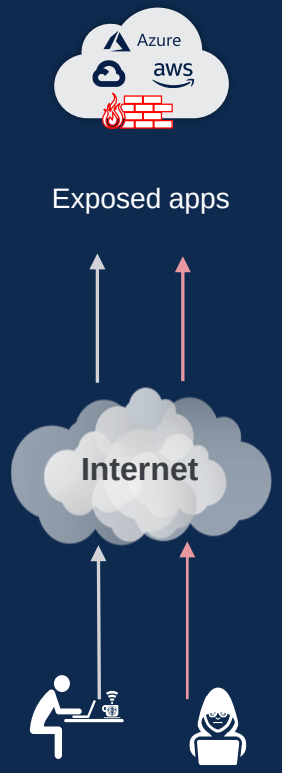
Minimize exposure by keeping applications invisible

If you publish your phone number



Good and bad guys can call you

If you publish apps on the internet (public cloud)



Apps can be attacked by bad guys

Unpublished number, AI-powered exchange service

Only good guys can call you

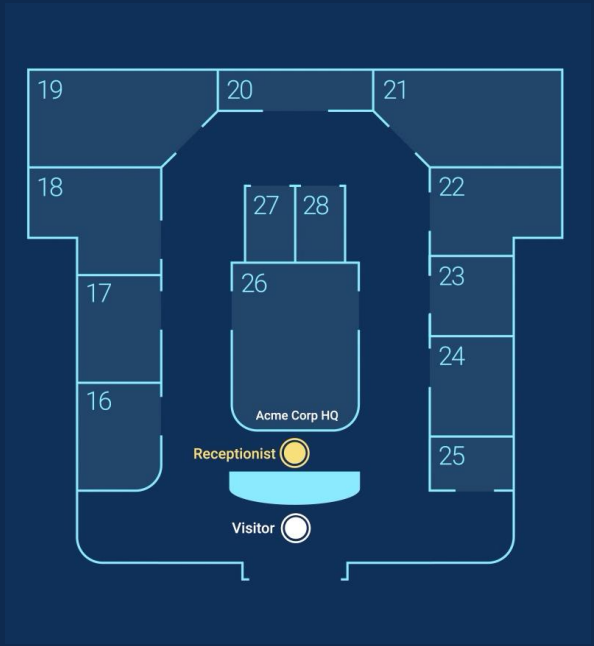
Unpublished apps, cloud as an exchange service

Only good guys can access apps For others they are invisible

Publishing apps on the internet using a traditional firewall increases your attack surface.
North-South Zero Trust Access makes your apps invisible and accessible only by authorized users.

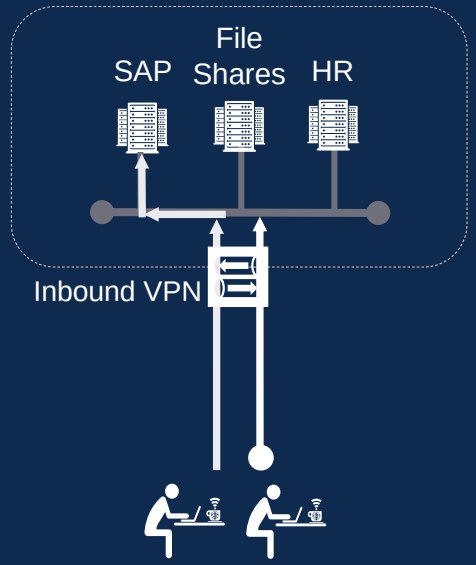
Enhance security by connecting users to applications

Unescorted office visitor



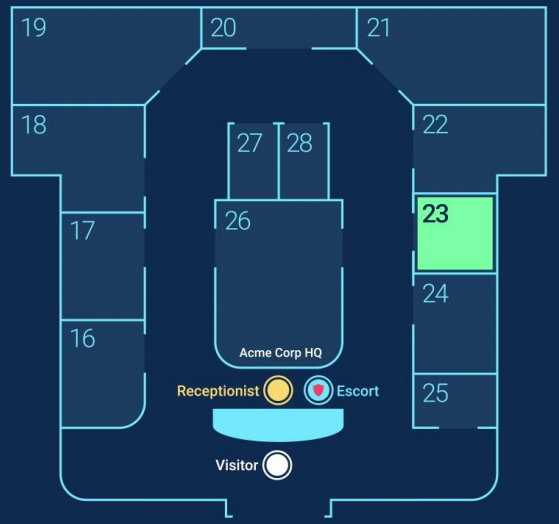
Strangers snooping = security risk

Connect a user to a network



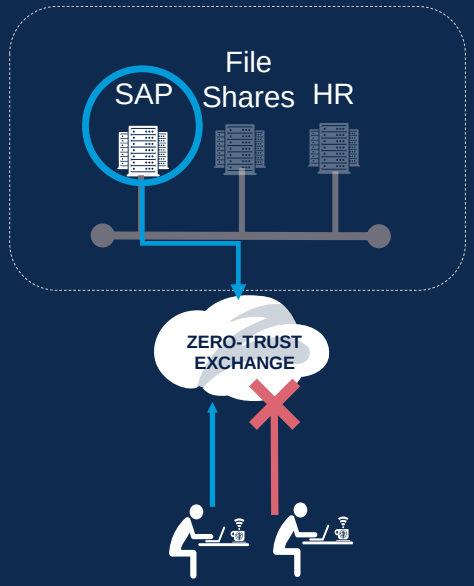
Network scanning = security risk

Escorting visitors to a meeting room



No snooping by strangers = better security

Connecting a user to an app (not a network)



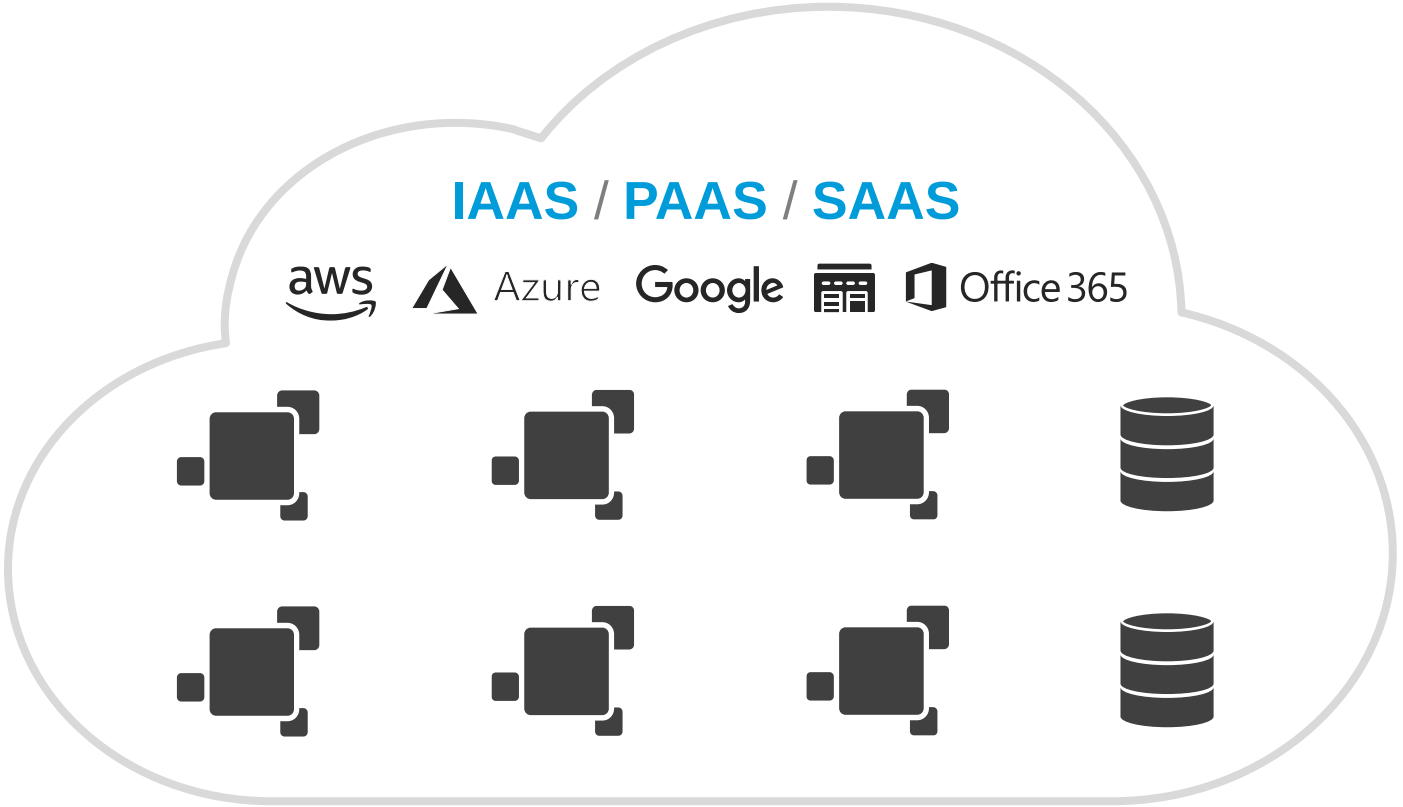
No scanning = better security

Unlike traditional VPN/FW, North-South Zero Trust Access connects a user to an app, not a network – better security

Simplifying security of the workload and platform

Gain Visibility

Discover assets and configurations

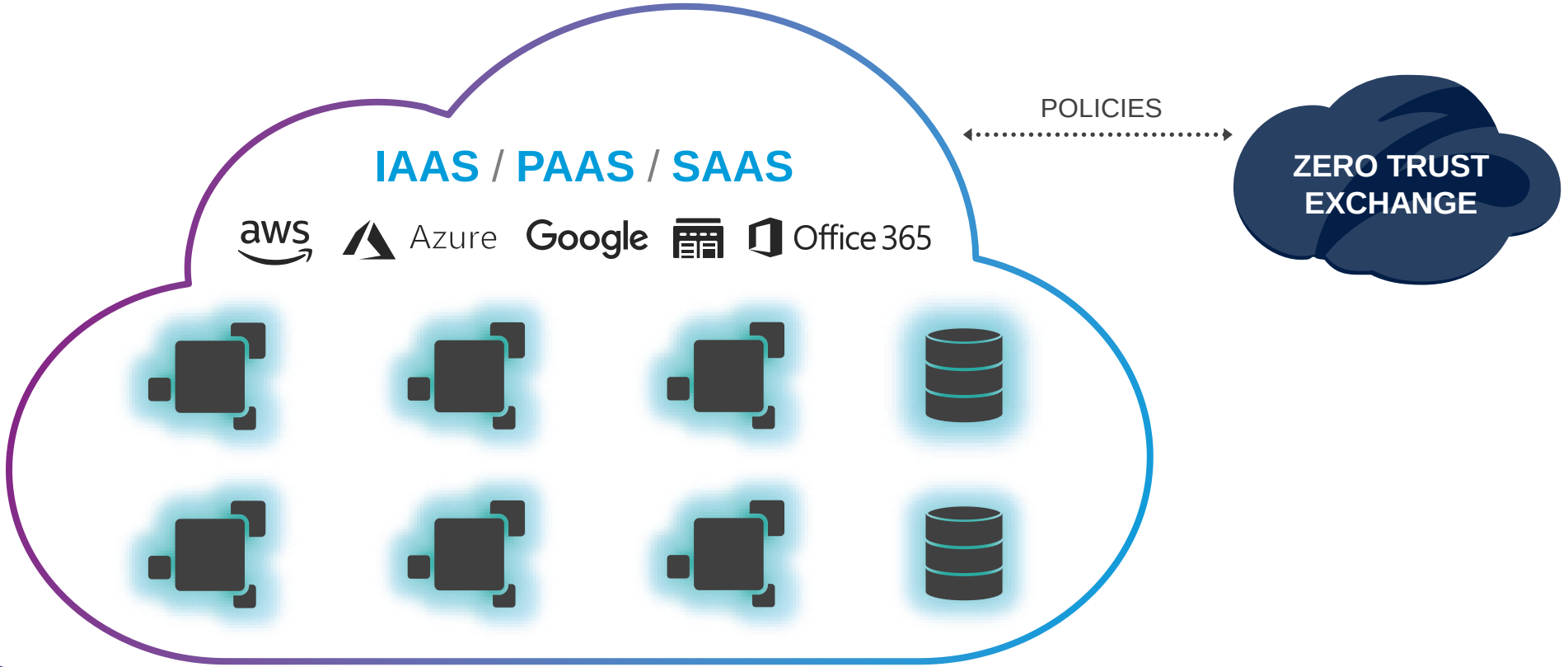


Simplifying security of the workload and platform

Gain Visibility → **Harden Platforms**

Discover assets and configurations

Remediate misconfigurations



POLICIES

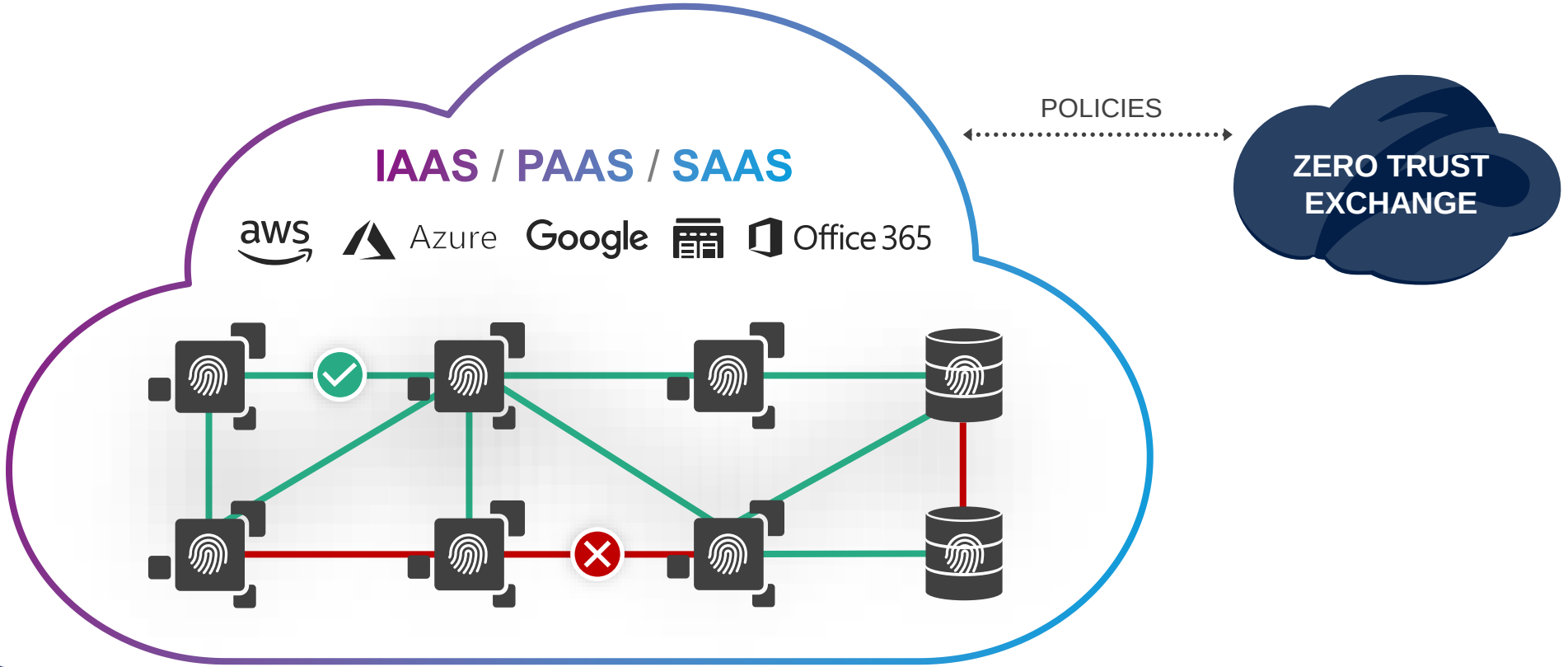
Simplifying security of the workload and platform

Gain Visibility → **Harden Platforms** → **Protect Workloads**

Discover assets and configurations

Remediate misconfigurations

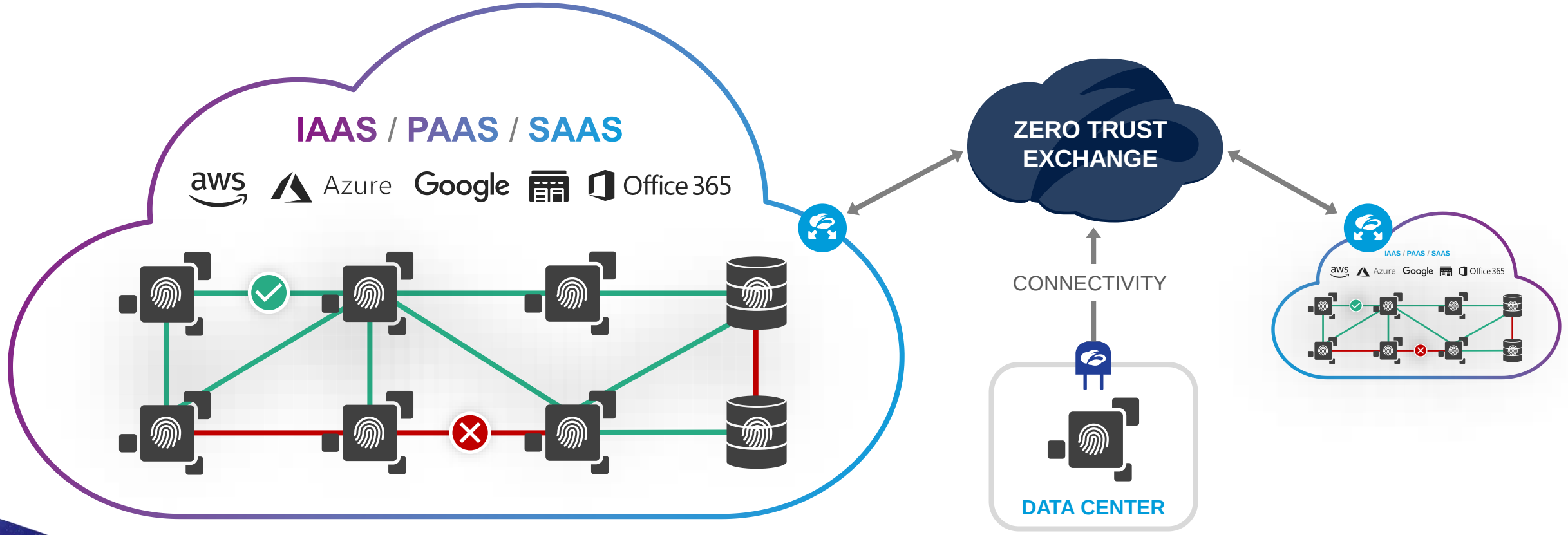
Verify software-identity before communication



POLICIES

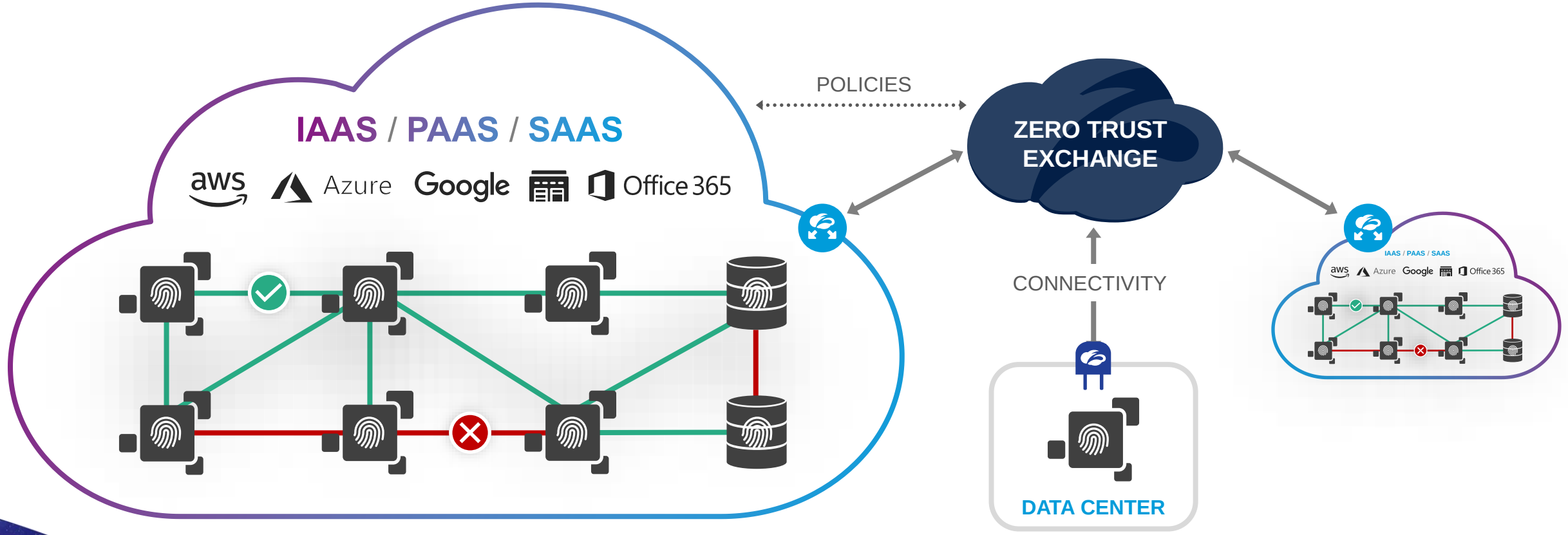
Simplifying security of the workload and platform

Gain Visibility	Harden Platforms	Protect Workloads	Secure Connectivity
Discover assets and configurations	Remediate misconfigurations	Verify software-identity before communication	**Secure access across multi-clouds and internet**



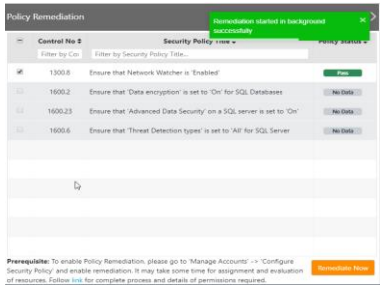
Simplifying security of the workload and platform

Gain Visibility	Harden Platforms	Protect Workloads	Secure Connectivity	Continuously Validate
Discover assets and configurations	Remediate misconfigurations	Verify software-identity before communication	Secure access across multi-clouds and internet	**Enforce least-privilege in dynamic environments**



Remediate cloud misconfigurations and compliance

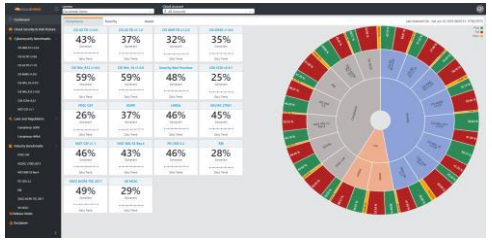
Cloud Security Posture Management (CSPM) offers continuous security assurance and remediation

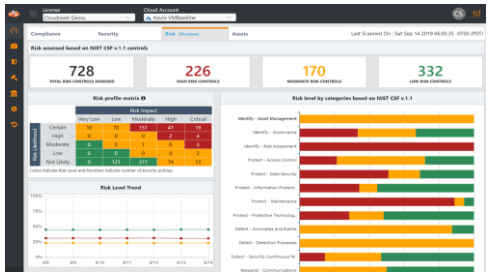


AUTO-REMEDIATE MISCONFIGURATIONS

IMMEDIATELY DISCOVER ASSETS AND CONFIGURATIONS

IDENTIFY NON-COMPLIANT CONFIGURATIONS

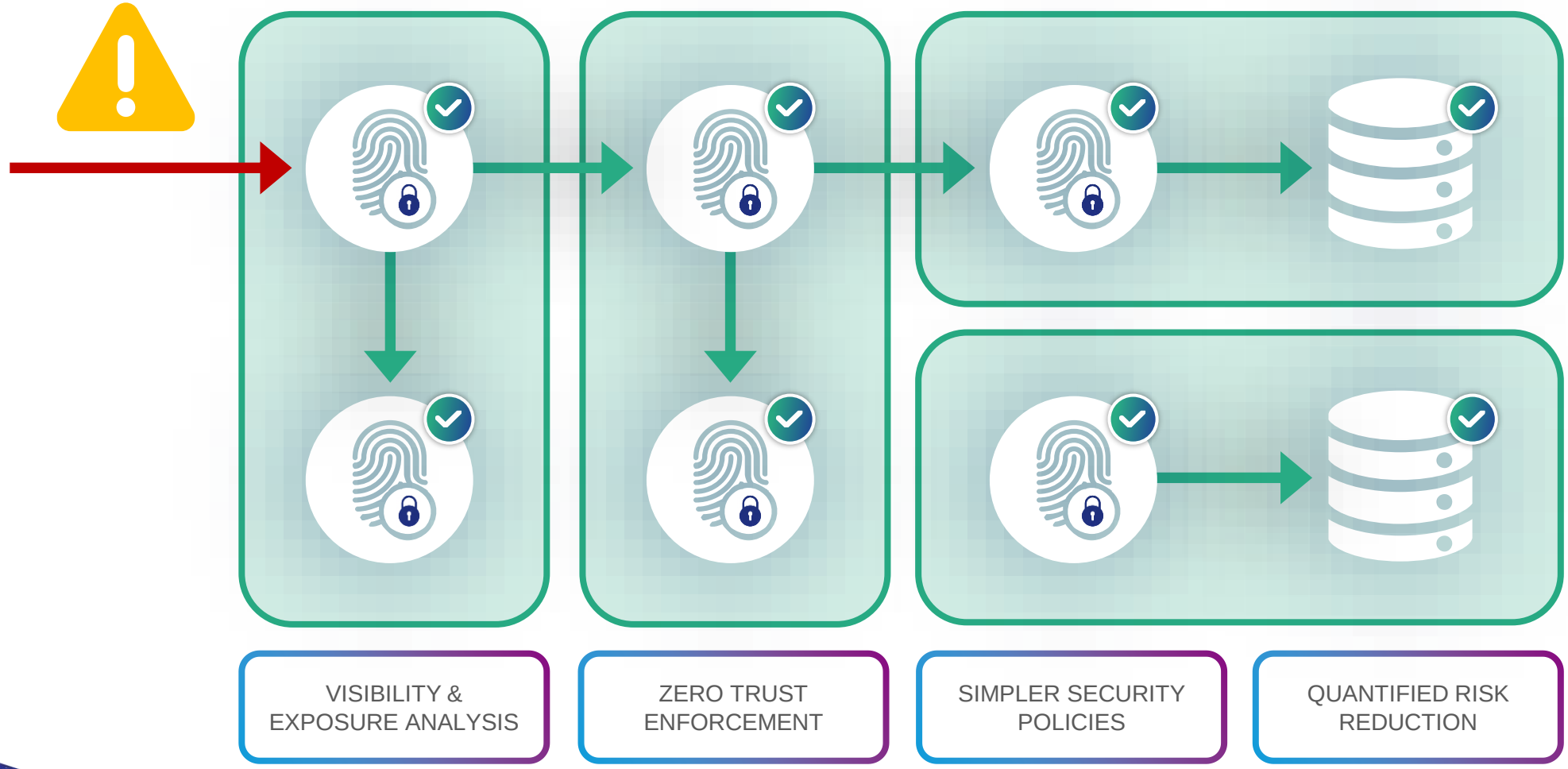




PRIORITIZE BASED ON RISK OF LIKELIHOOD AND IMPACT

Protect workloads easily using identity

Workload Segmentation provides identity-based microsegmentation, delivered through automation



Simple, secure cloud app access to internet, multi-cloud

East-West Zero Trust Access provides secure connectivity with automated deployment

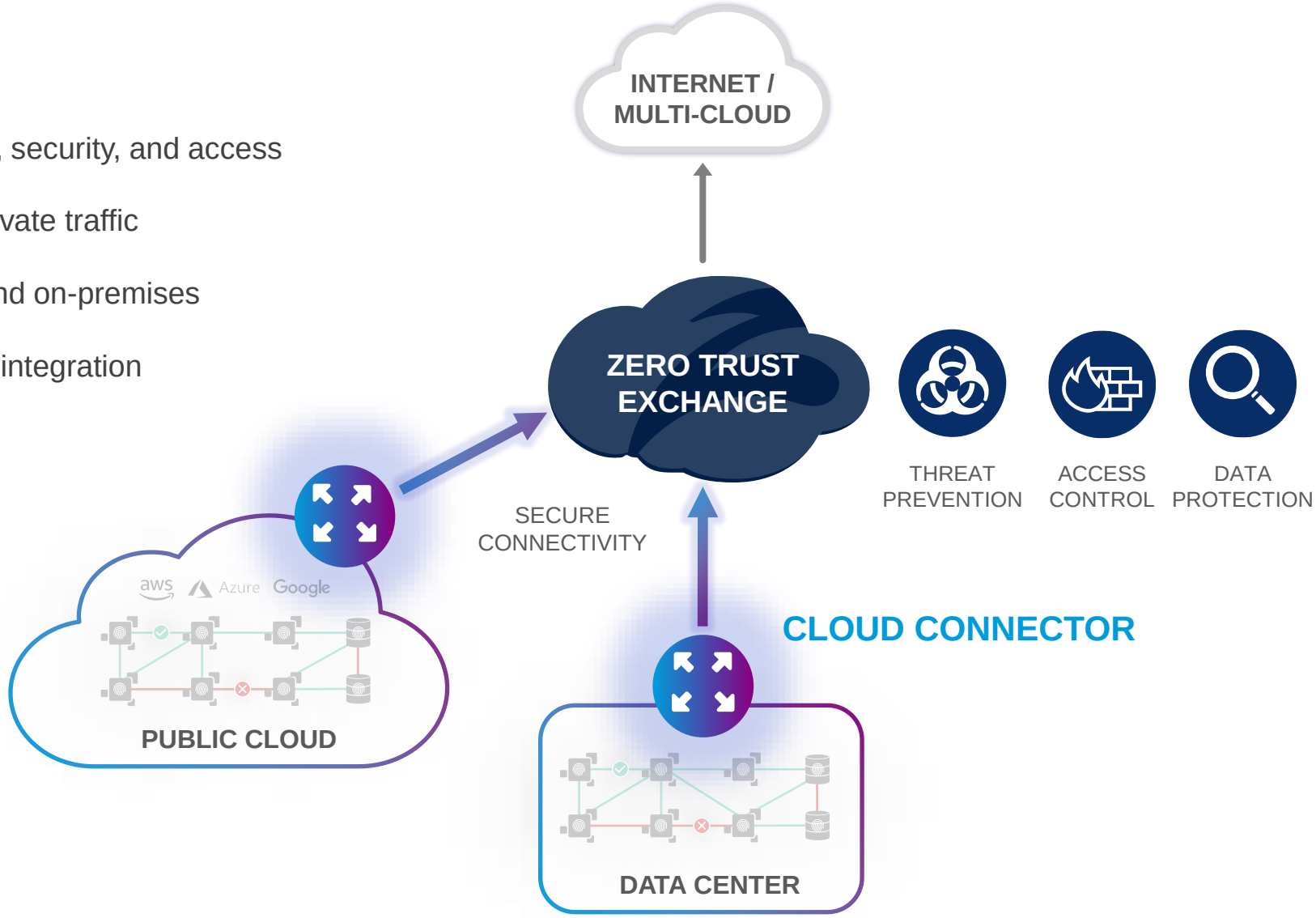
Integrated connectivity and security

Unified control plane – traffic forwarding, security, and access

Flexible traffic steering – internet and private traffic

Automated deployment – public cloud and on-premises

Deep visibility – detailed logs and SIEM integration



Best practices for enabling DevSecOps

Culture and politics

- Get executive-level buy-in
- Address cultural obstacles and silos
- Promote security as a shared responsibility
- Engage with progressive thought leaders

Skillsets and process

- Cross-train staff on DevOps and application security best practices
- Understand and leverage the new DevSecOps abstraction model
- Create defined insertion points for zero trust security in the DevOps toolchain

Technology

- Take applications off the network
- Protect workloads using identity
- Continuously validate security

Cloud-enabled technologies support agile application development and deployment with robust application security

How to eat the elephant

- First Day
  - Engage with stakeholders on creating alignment among DevOps and security teams and processes
  - Assess the state of current application security processes with current and planned applications
- 30 Days
  - Establish joint groups of DevOps and security personnel to break down silos
  - Cross-educate both security and DevOps on the benefits of taking apps off the network
  - Evaluate the use of zero trust security, identity-based microsegmentation, and cloud security posture management
- 90 Days
  - Adopt zero trust security, identity-based microsegmentation, and cloud security posture management
  - Establish processes whereby new and existing applications are automatically provisioned within the Zero Trust Exchange