
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV



PRT073

SPONSORED BY ZSCALER

Zero Trust CNAPP and cloud workload protection with Zscaler

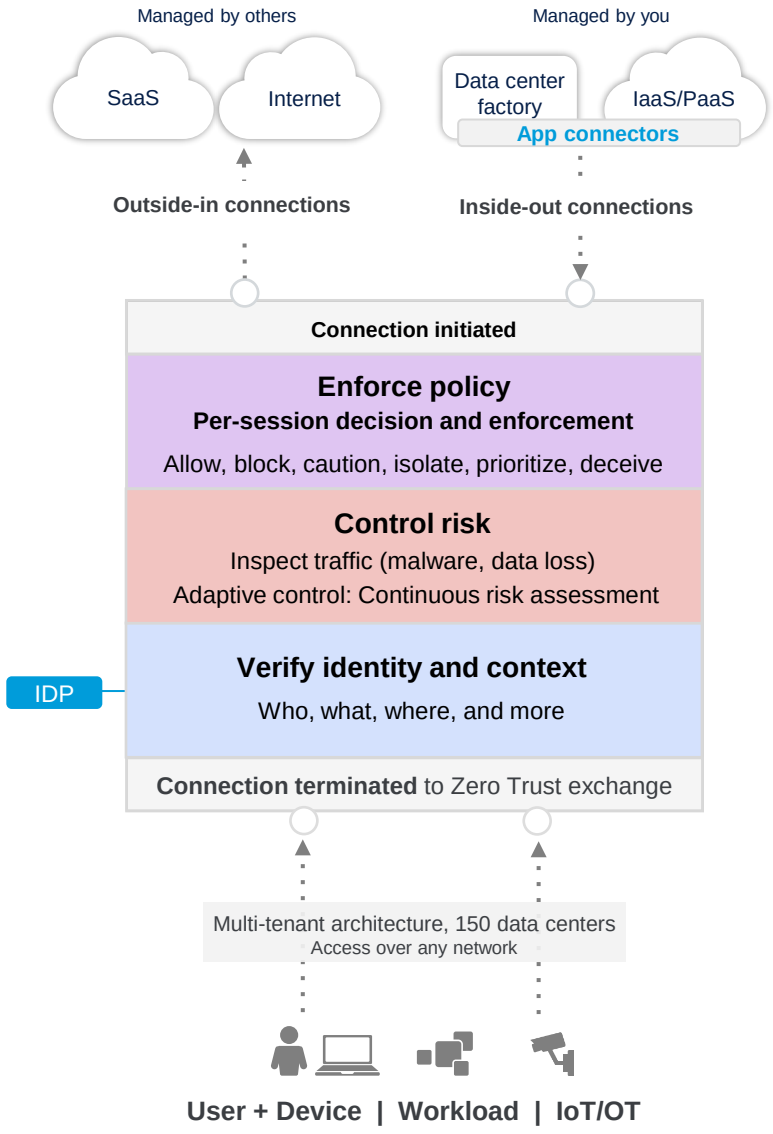
David Sedgwick

Field CTO
Zscaler



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

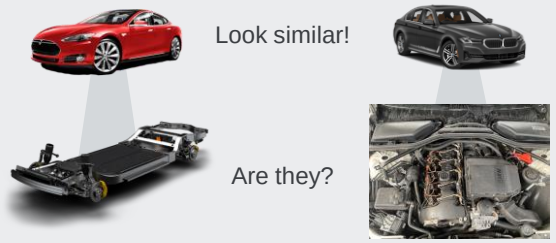
Zscaler Zero Trust exchange architecture

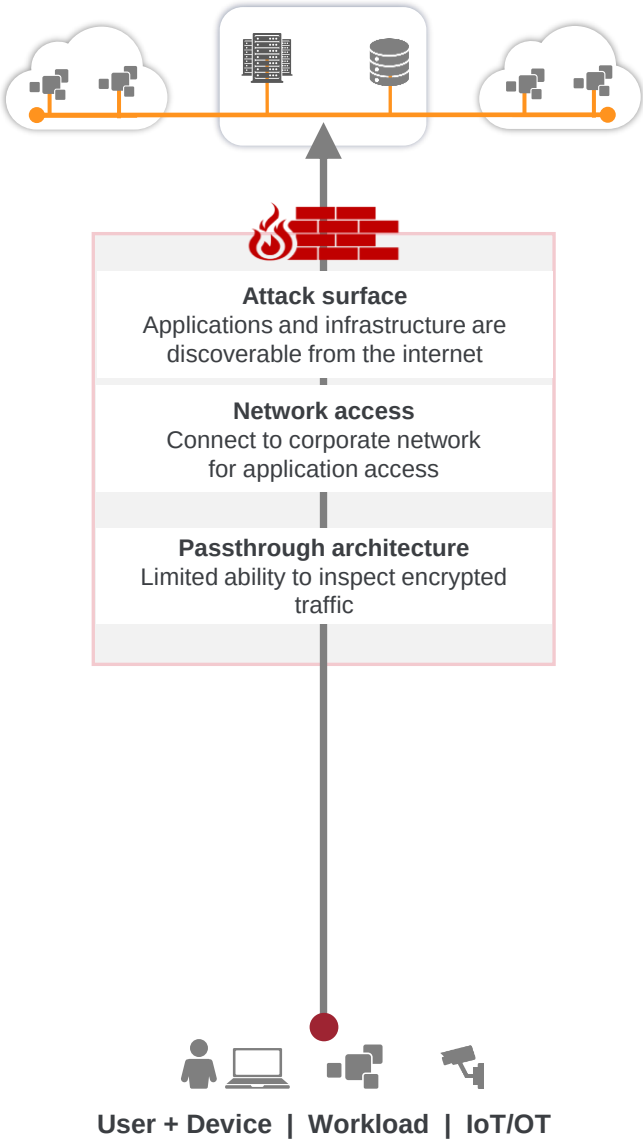


Zero Trust		Firewalls/VPN
●	**Minimize attack surface** No inbound connections, apps invisible	✕
●	**Prevent lateral movement** Connect to apps, not networks	✕
●	**Prevent compromise and data loss** Proxy architecture, SSL/TLS inspection	◒

You can't do Zero Trust security with firewalls/VPN

What's the difference between these two cars?

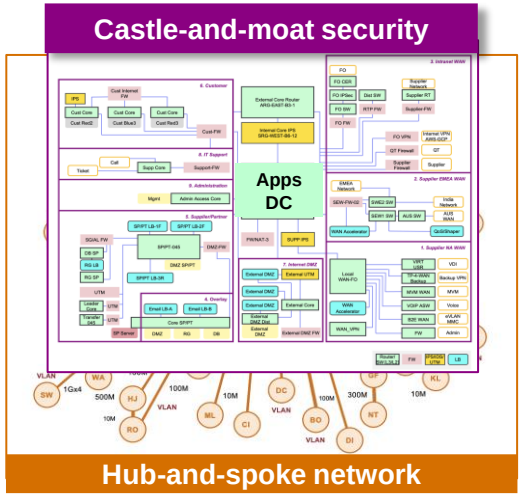


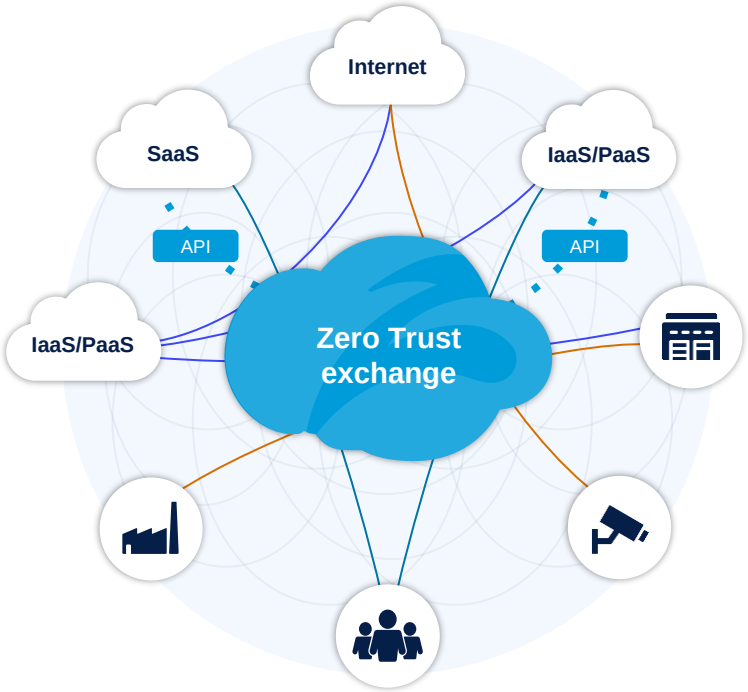


© 2022 Zscaler, Inc. All rights reserved.

Zscaler platform offerings

Comprehensive and integrated Zero Trust platform enables security and network transformation





Zscaler for users

- Secure internet and SaaS access (ZIA)
- Secure private app access (ZPA)
- Digital experience (ZDX)

Zscaler for workloads

- Secure internet access
- Secure workload-to-workload communication
- Configuration and exposure scanning (CNAPP)

Zscaler for IoT/OT

- Secure internet, SaaS, private app access
- Privileged access to OT

A comprehensive cloud security platform that eliminates multiple point products and reduces business risk

© 2022 Zscaler, Inc. All rights reserved.

Zscaler for workloads: Build and run secure cloud applications

Workload exposure scanning

Identify attack surface

Remediate vulnerabilities

Secure data

Cloud configuration scanning

IaC security

Posture management

Entitlements management

Workload-to-internet runtime protection

Prevent compromise

Prevent data loss

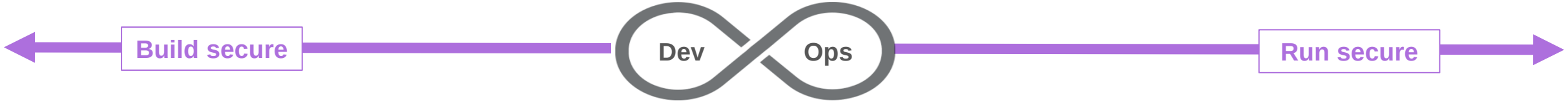
Workload-to-workload ZTA

Identify attack surface

Prevent lateral movement

Posture control

Workload communications





Efficiency via native guardrails in dev & DevOps tools



Enforce immutability by eliminating configuration drift



Agentless deployment for 100% workload coverage



Zero Trust architecture eliminates attack surface



Zero Trust exchange platform trusted by 6,000+ enterprises

© 2022 Zscaler, Inc. All rights reserved.

Zscaler for workloads: Posture control

Workload exposure scanning

Identify attack surface

Remediate vulnerabilities

Secure Data

Cloud configuration scanning

IaC security

Posture management

Entitlements management

Workload-to-internet runtime protection

Prevent compromise

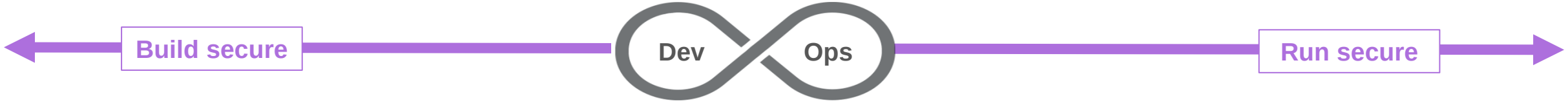
Prevent data loss

Workload-to-workload ZTA

Identify attack surface

Prevent lateral movement

Posture control — **Workload communications**





Efficiency via native guardrails in dev & DevOps tools



Enforce immutability by eliminating configuration drift



Agentless deployment for 100% workload coverage



Zero Trust architecture eliminates attack surface



Zero Trust exchange platform trusted by 6,000+ enterprises

© 2022 Zscaler, Inc. All rights reserved.

Cloud innovation models have introduced new security challenges

Dynamic, automated environments

Rapidly expanding cloud workloads



Hundreds (400+) of cloud services used



Multiple cloud platforms to manage



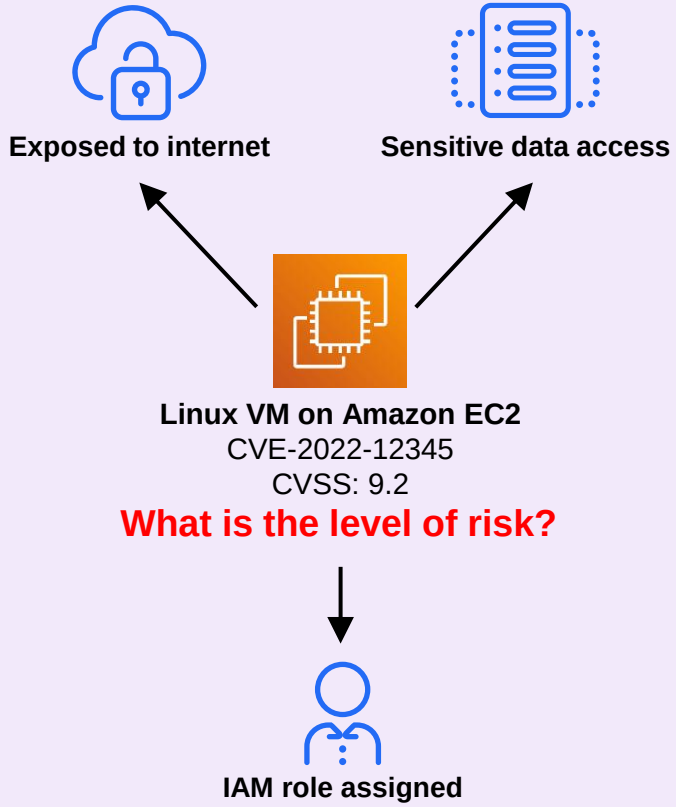
Many dev, DevOps, security stakeholders



Too many alerts, too late – Slows resolution

- **Data loss prevention** — 921
- **Container/serverless security** — 97
- **Vulnerabilities and exposure** — 641
- **CIEM** — 211
- **CSPM** — 785
- **Asset inventory/CMDB**

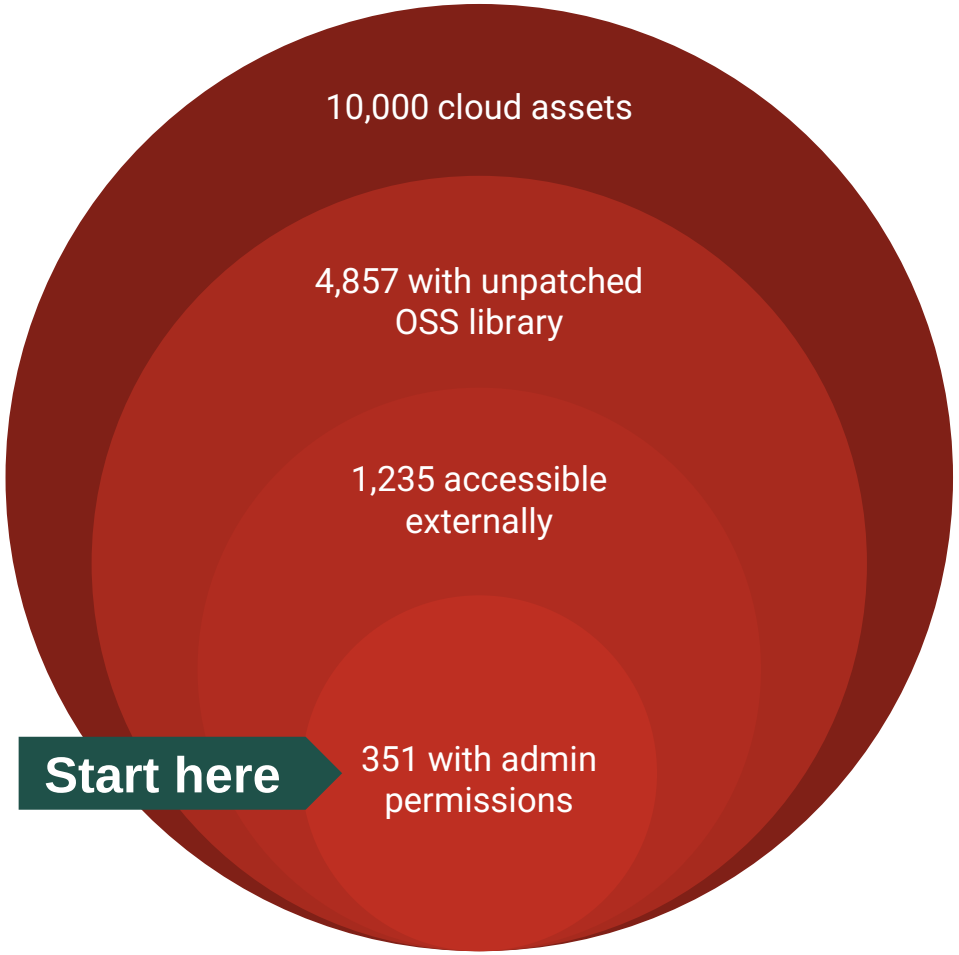
Difficult to prioritize true cloud risk



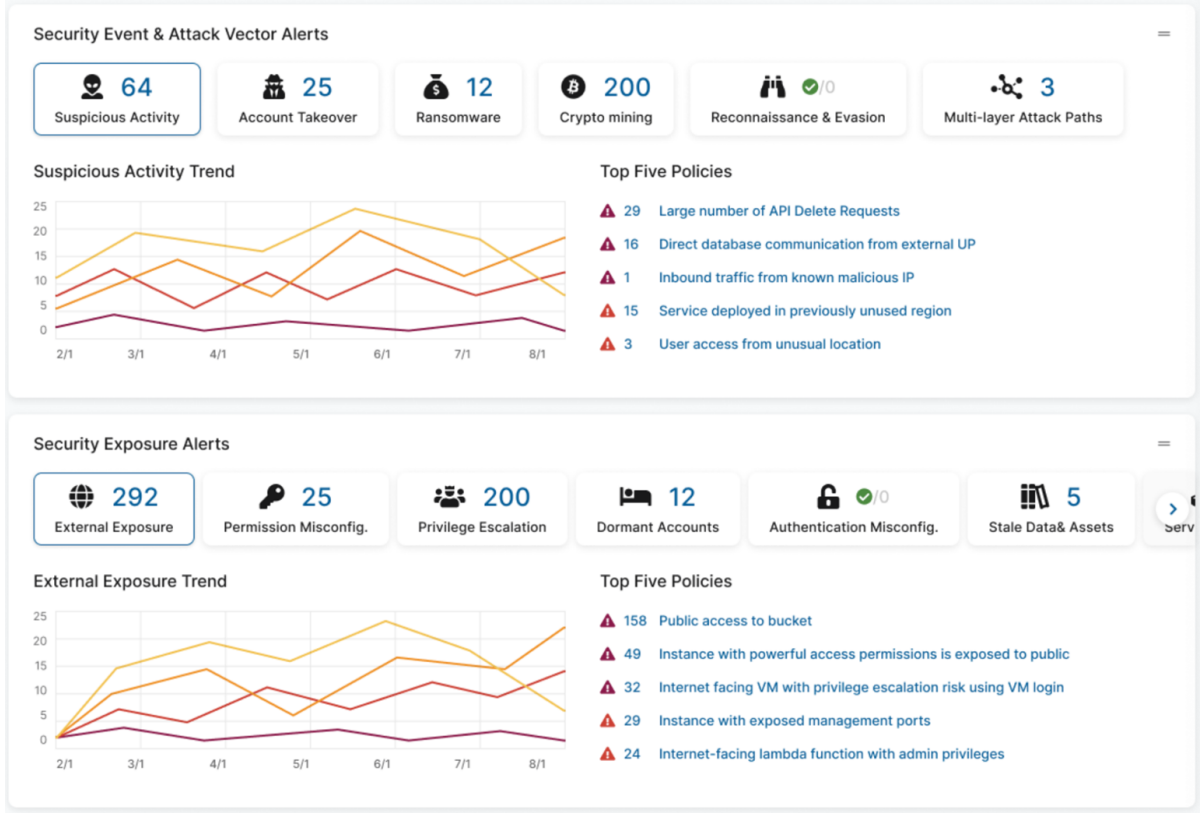
© 2022 Zscaler, Inc. All rights reserved.

Correlating and prioritizing cloud threats and risks with CNAPP

CNAPP in action: Critical CVE reported in open-source library

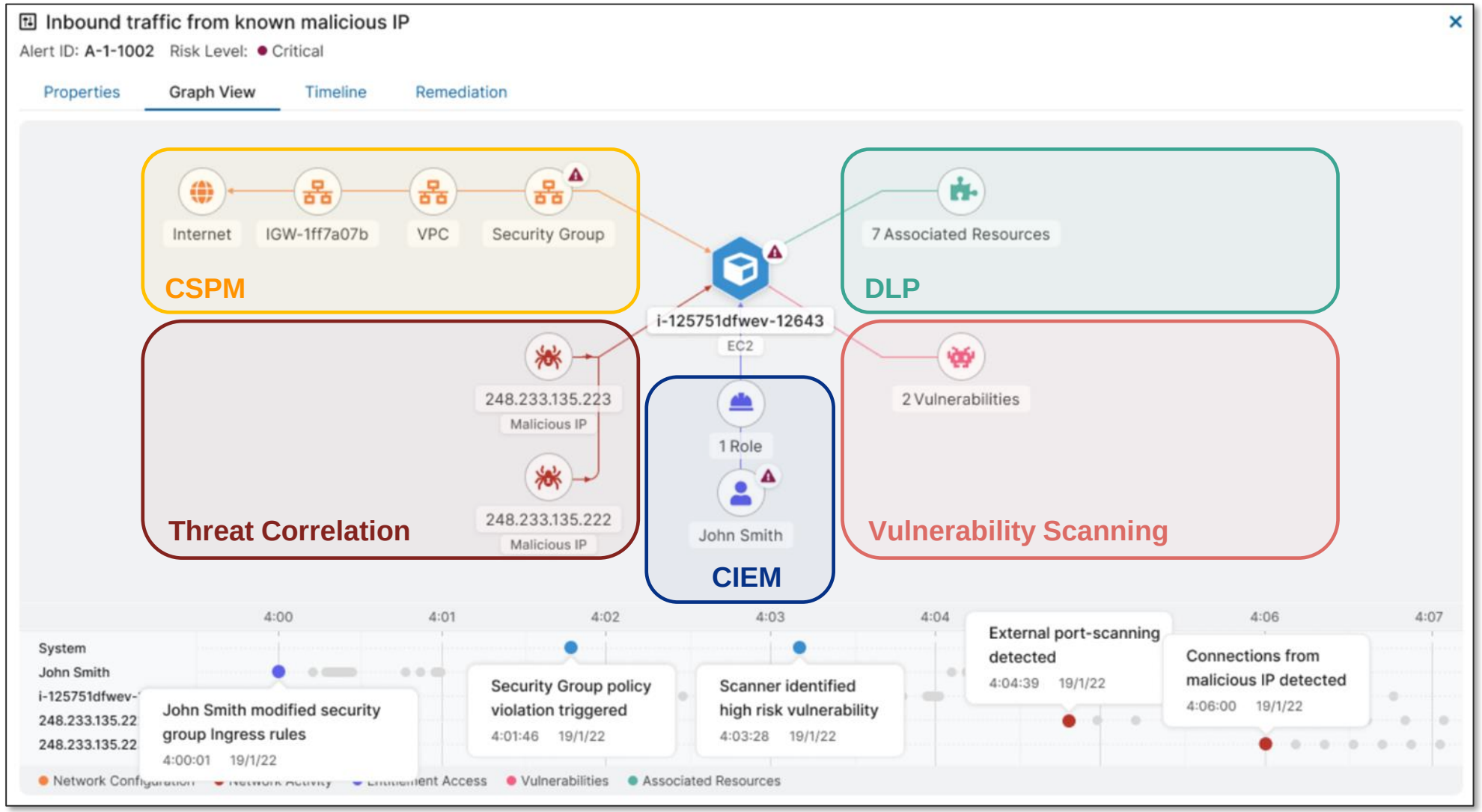


Prioritized risks and incidents



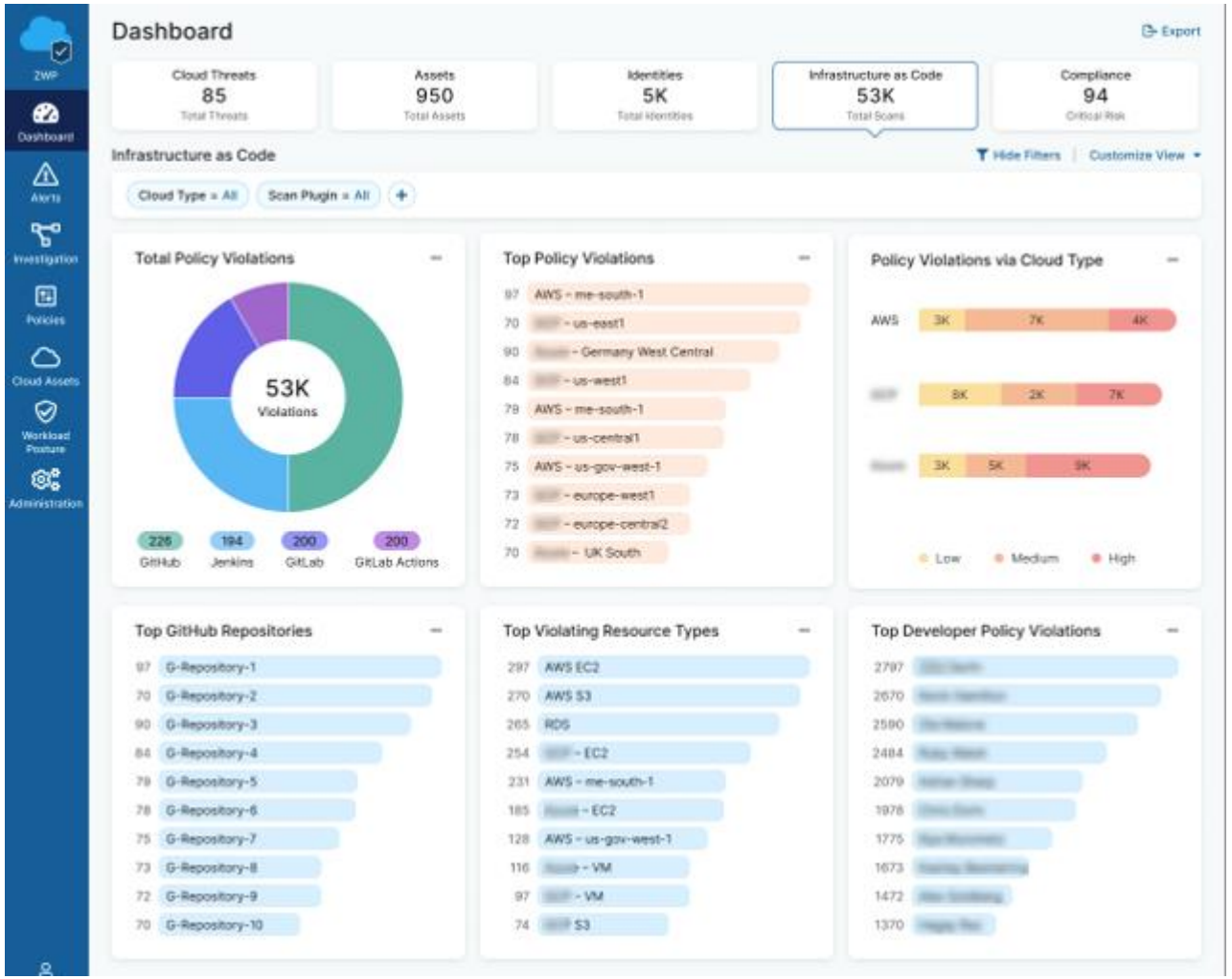
© 2022 Zscaler, Inc. All rights reserved.

Investigating multi-part risks and incidents quickly and easily



© 2022 Zscaler, Inc. All rights reserved.

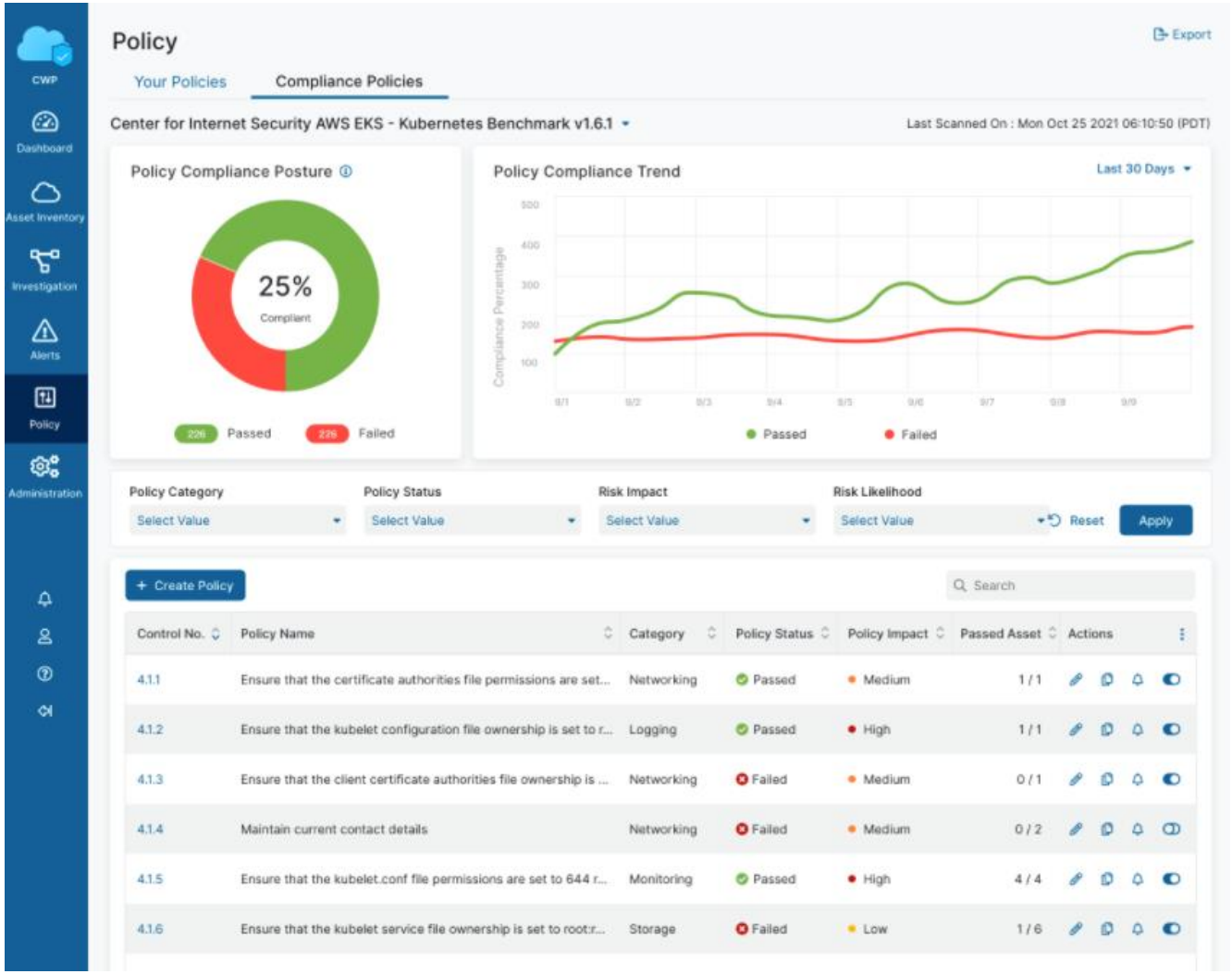
Shift left to identify exposures before deployment



- Native tool integration and experience fosters dev/DevOps collaboration with Security teams
  - IDEs
  - Version control systems
  - CI/CD tools
- Scanning flexibility for diverse enterprises
  - Terraform
  - AWS CloudFormation
  - Azure Resource Manager (ARM)
  - Kubernetes YAML/Helm charts
  - Docker files

© 2022 Zscaler, Inc. All rights reserved.

Continuously validate compliance



- MITRE ATT&CK mapping
- Security frameworks
  - CIS
  - CSA CCM
- Industry regulations
  - PCI DSS, NIST CSF, HIPAA, ISO 27001, SOC 2, NIST 800-53
- Regional regulations
  - GDPR
- Customer-defined custom policy rules and framework mapping

© 2022 Zscaler, Inc. All rights reserved.

Zscaler for workloads – Workload communications

Workload exposure scanning

Identify attack surface

Remediate vulnerabilities

Secure data

Cloud configuration scanning

IaC security

Posture management

Entitlements management

Workload-to-internet runtime protection

Prevent compromise

Prevent data loss

Workload-to-workload ZTA

Identify attack surface

Prevent lateral movement

Posture control — **Workload communications**

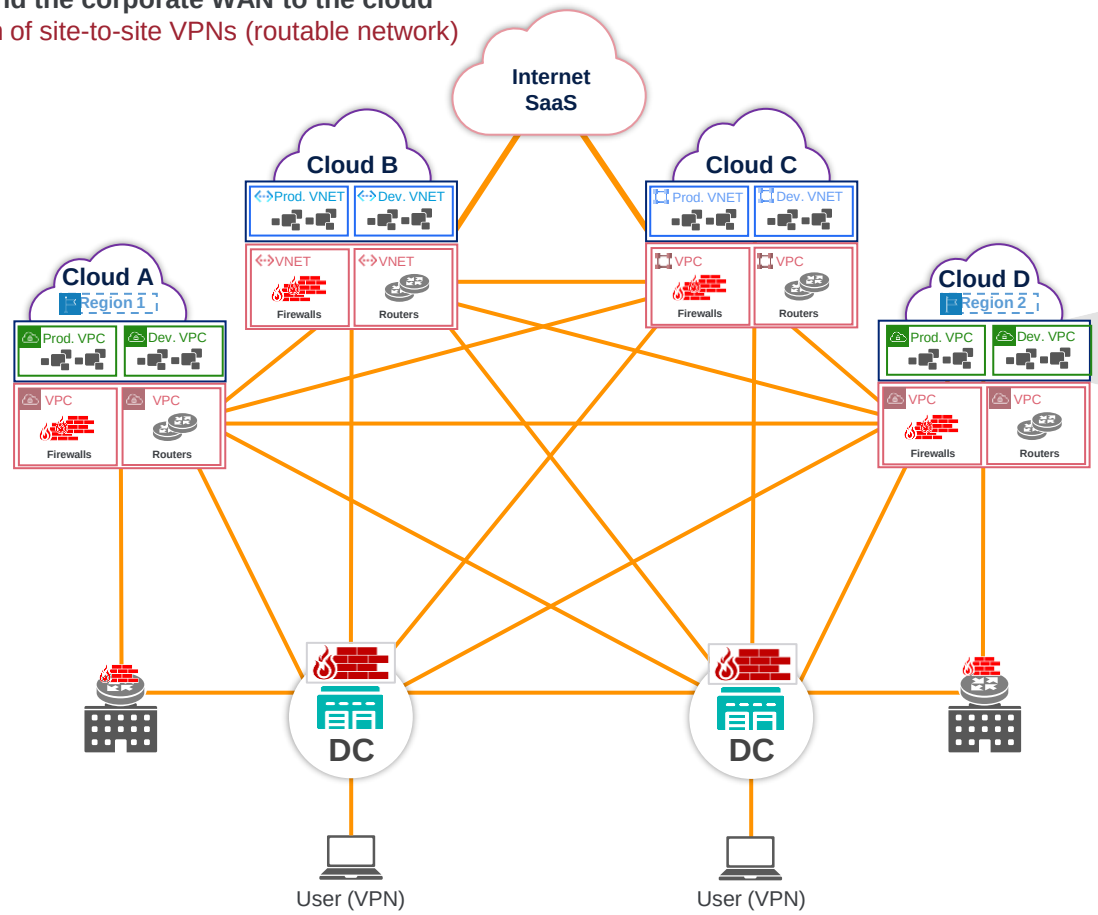
Build secure — Dev Ops — Run secure

- Efficiency via native guardrails in dev & DevOps tools
- Enforce immutability by eliminating configuration drift
- Agentless deployment for 100% workload coverage
- Zero Trust architecture eliminates attack surface
- Zero Trust exchange platform trusted by 6,000+ enterprises

© 2022 Zscaler, Inc. All rights reserved.

Extending a legacy network and security to the public cloud

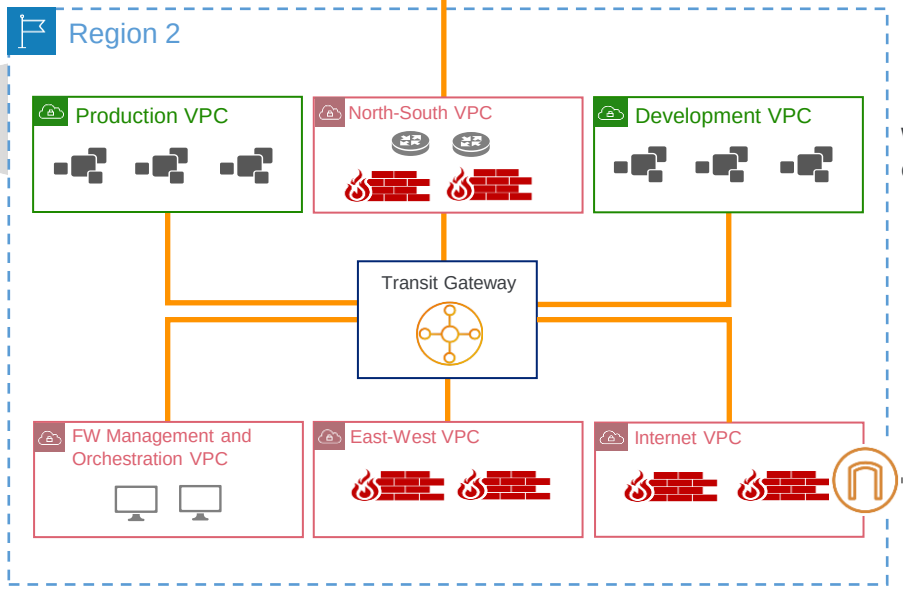
Extend the corporate WAN to the cloud
A mesh of site-to-site VPNs (routable network)



Increased risk of lateral threat movement
A single infected workload can infect everything on the network

Broadened internet attack surface
Every internet-facing firewall can be discovered and exploited

Workload communications to other AWS Regions, data centers, public clouds



Workload-to-workload communication

Workload-to-internet communication

FW VM bloat (+ squid proxies for cyberthreat and data protection)

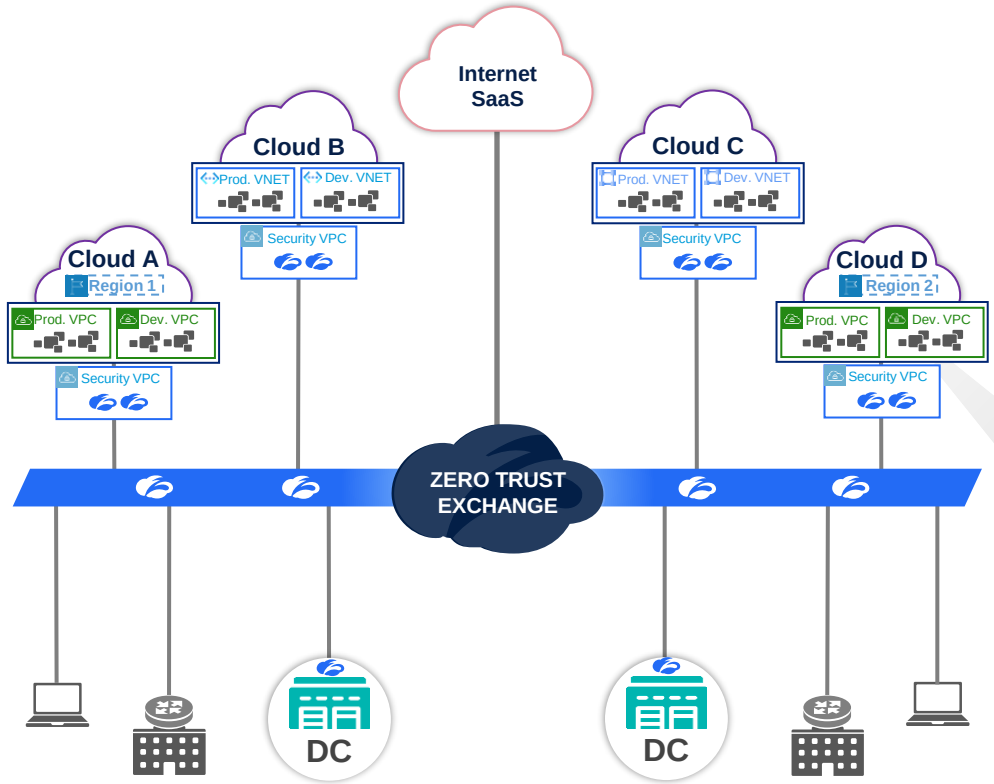
Routing complexity (IP overlap/conflict)

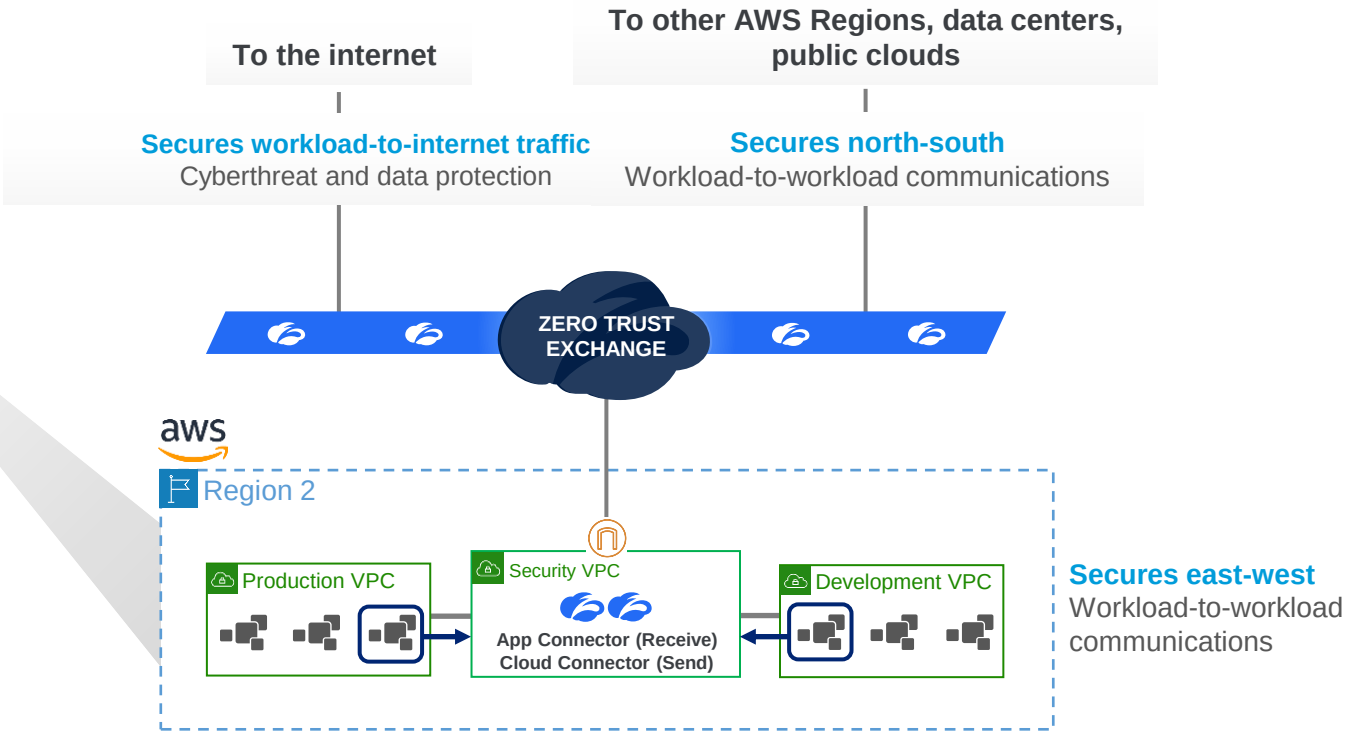
Unmanageably complex and expensive
Replicating DMZs across clouds, Regions, and Availability Zones
High cost of connecting everything with a mesh network

© 2022 Zscaler, Inc. All rights reserved.

With Zero Trust cloud connectivity, you don't extend your WAN

Secure workload-to-workload communications over any network (non-routable network)



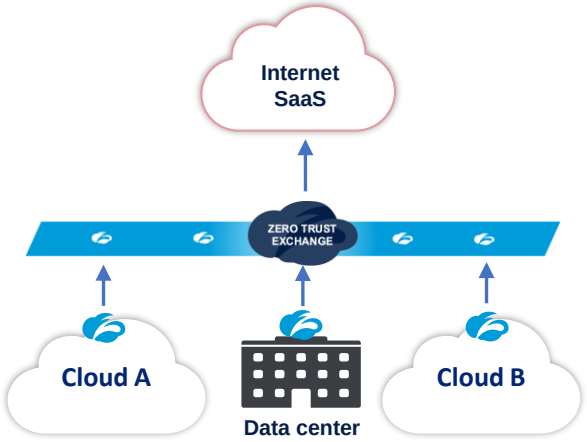


- **Eliminates the risk of lateral threat movement**
  Native workload-to-workload segmentation over any network
- **Eliminates the internet attack surface**
  Applications are not discoverable on the internet
- **Eliminates VM bloat (FWs, squid proxies, routing)**
- **Eliminates routing complexity (no IP overlap issues)**
- **Reduces operational complexity and cost**
  Eliminates the need for virtual DMZs and a mesh of site-to-site VPNS

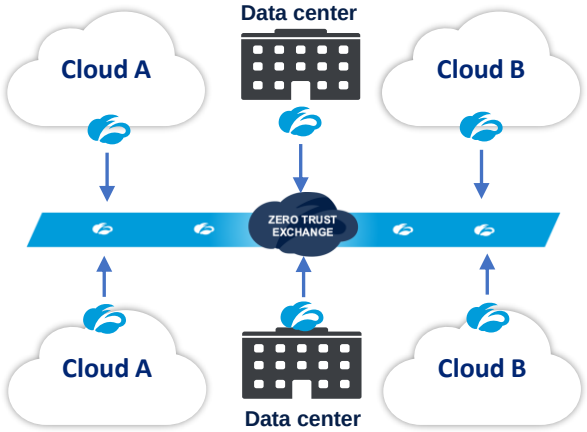
© 2022 Zscaler, Inc. All rights reserved.

Securing workload connectivity with Zero Trust: Three use cases

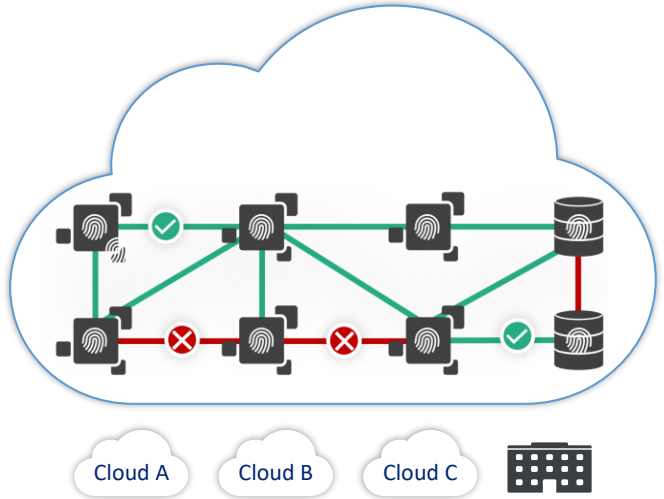
1 Workload-to-internet



2 Workload-to-workload across clouds



3 Workload-to-workload within VPCs/data centers



Attack surface elimination

- No inbound connections to applications
- Non-routable network between cloud and data center

Data and cyberthreat protection

- Stop sophisticated threats such as ransomware, phishing, zero days
- SSL inspection at scale

No lateral threat movement

- Identity-based segmentation at individual process level
- Removes unnecessary paths, protects what's needed

Reduced costs and complexity

- Eliminate virtual firewalls, VPN transit gateways, peering configurations
- Eliminate management appliances and reduce VM bloat

© 2022 Zscaler, Inc. All rights reserved.

Zscaler for workloads: Build and run secure cloud applications

Workload exposure scanning

Identify attack surface

Remediate vulnerabilities

Secure data

Cloud configuration scanning

IaC security

Posture management

Entitlements management

Workload-to-internet runtime protection

Prevent compromise

Prevent data loss

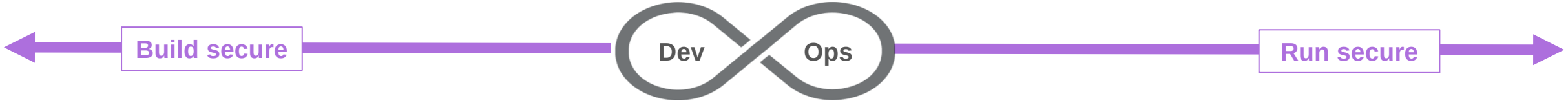
Workload-to-workload ZTA

Identify attack surface

Prevent lateral movement

Posture control

Workload communications





Efficiency via native guardrails in dev & DevOps tools



Enforce immutability by eliminating configuration drift



Agentless deployment for 100% workload coverage



Zero Trust architecture eliminates attack surface



Zero Trust exchange platform trusted by 6,000+ enterprises

© 2022 Zscaler, Inc. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.