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

PRT202

SPONSORED BY CISCO

It's an application-first world: Shouldn't your cloud security match?

Justin Buchanan

Sr. Director, Product Management
Cisco

aws

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

CISCO
SECURE

It is an application first world.

Shouldn’t your cloud security match?

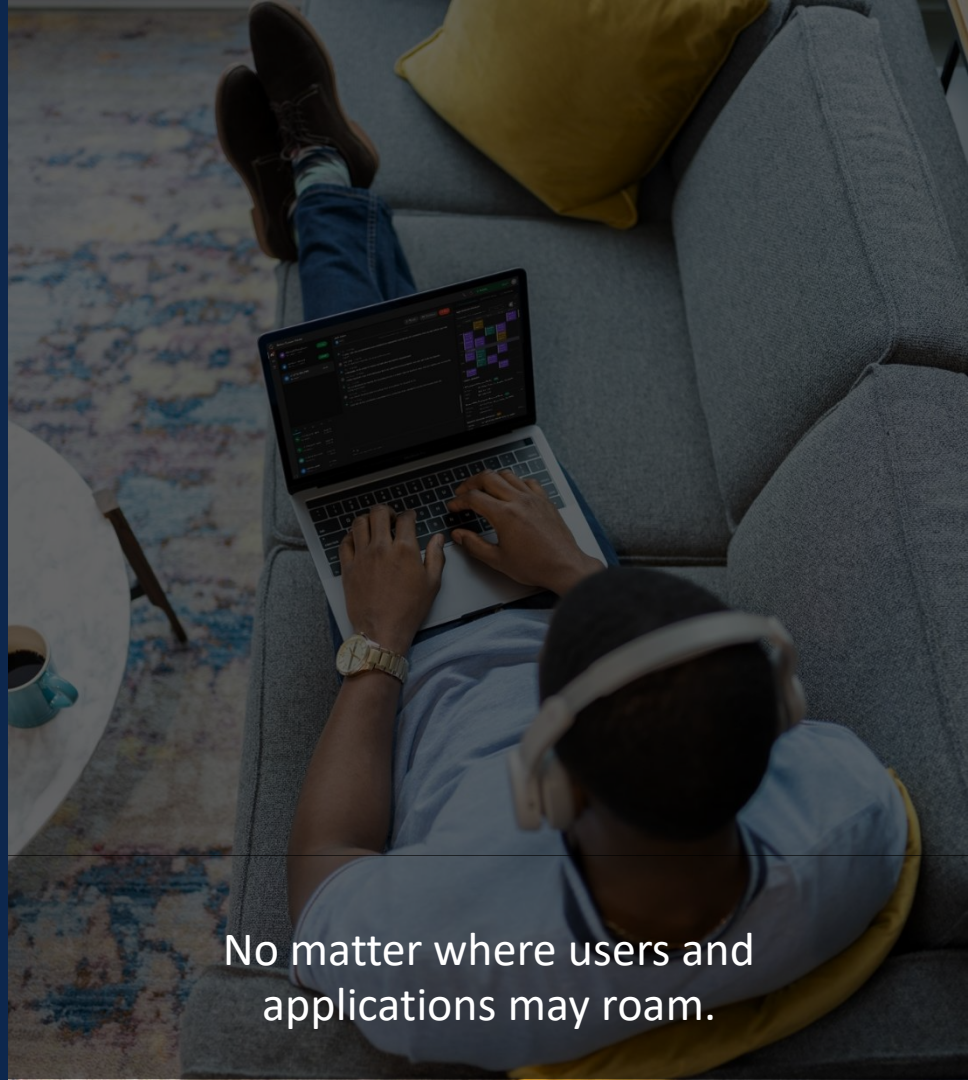
Justin Buchanan
Sr. Director, Product Management

Agenda



- The rapid expansion of the network
- Where is my perimeter?
- Flip the model
- Micro-segmentation
- What about the user? A look at unifying policy
- AWS Control Tower

Business success depends on secure connected experiences.



cisco SECURE

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

New challenges for hybrid infrastructures

Old ways don’t work – So we are told



Hybrid Access

Permitter is gone with distributed users and applications



Old Security Ways

Don’t provide visibility and control and are being replaced with ZTNA



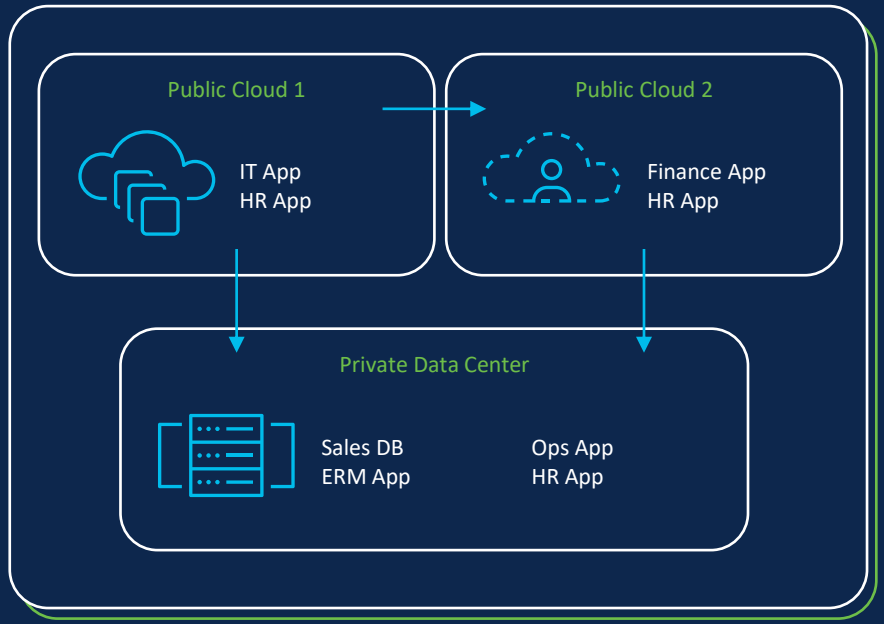
Rate of change

Containers and applications are spun up overnight across multiple environments

The world operates with data & apps living everywhere… And connected

82% of IT leaders have adopted hybrid cloud[1]

47% of IT leaders are deploying 2 to 3 public IaaS clouds[1]

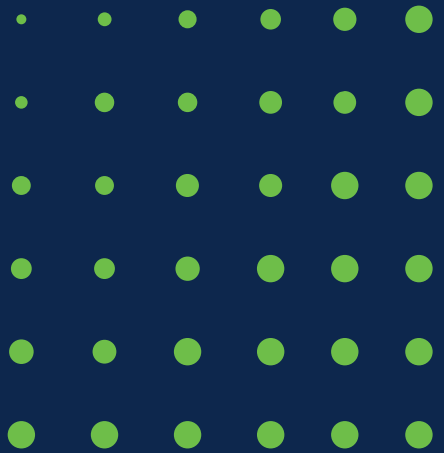


- If its's connected it can be protected by the network

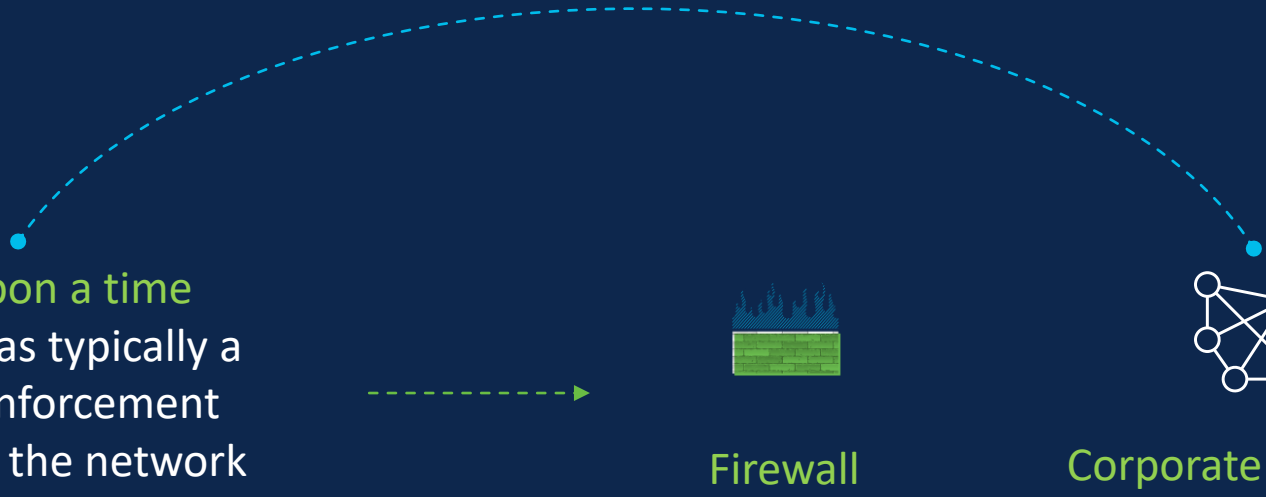
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

[1] 2022 Cisco Global Hybrid Cloud Trends Report

Where is the perimeter?



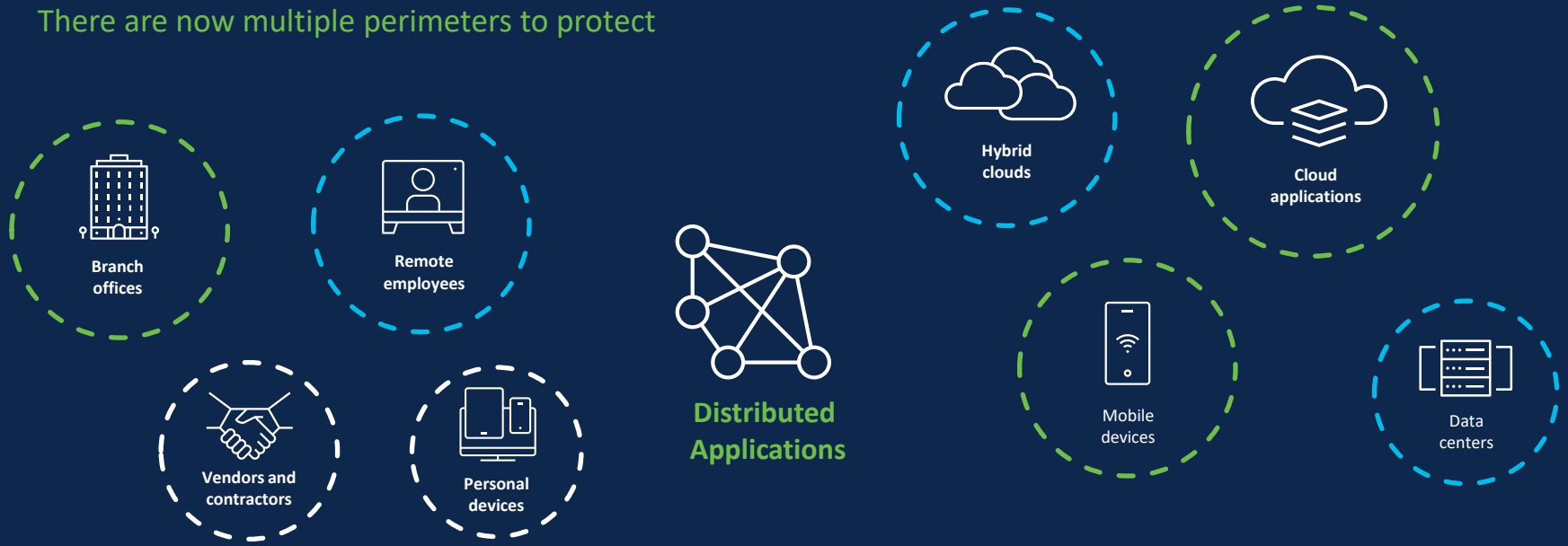
Why do we believe the permitter vanished?



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

But… It is still there

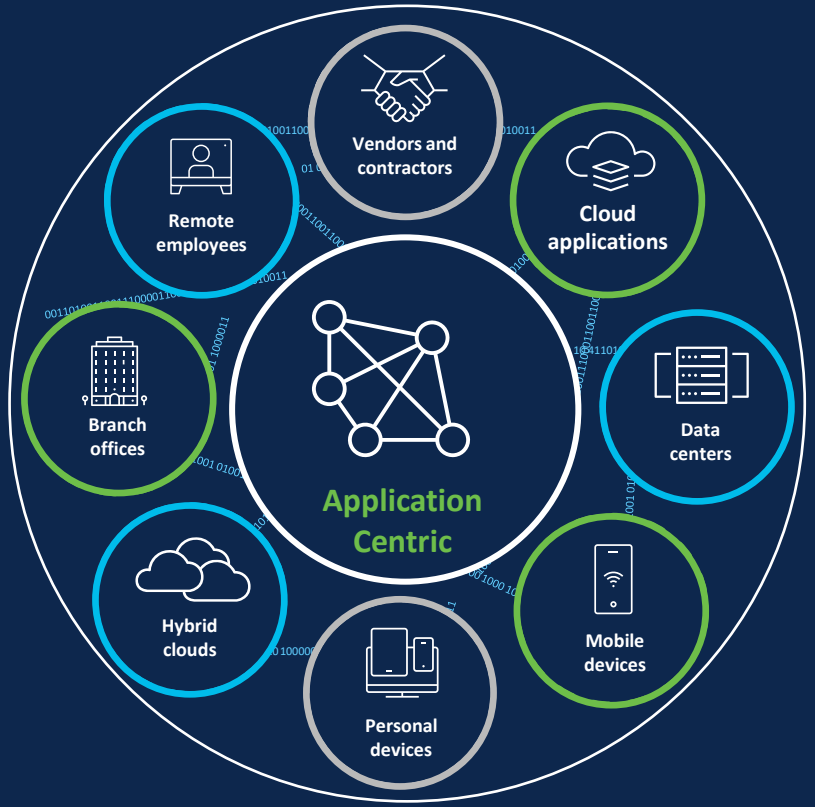
There are now multiple perimeters to protect



… as a result, the typical environment now requires numerous enforcement points

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

It’s time to flip the model



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Controlling access to distributed apps

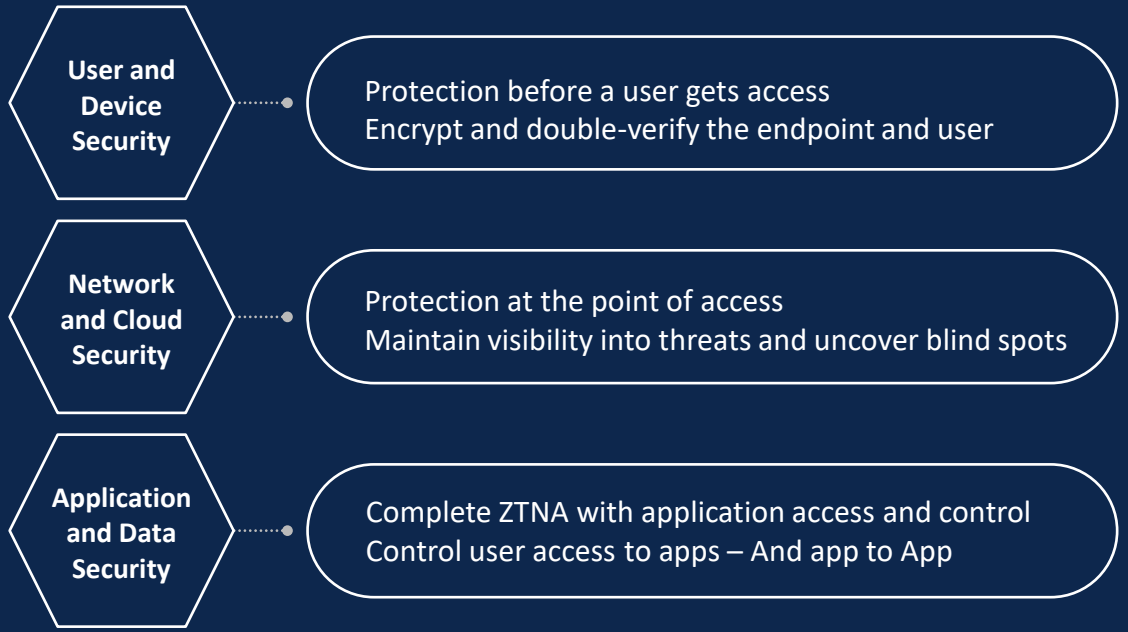
We often take a liner and siloed approach



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Manage access across three permitters

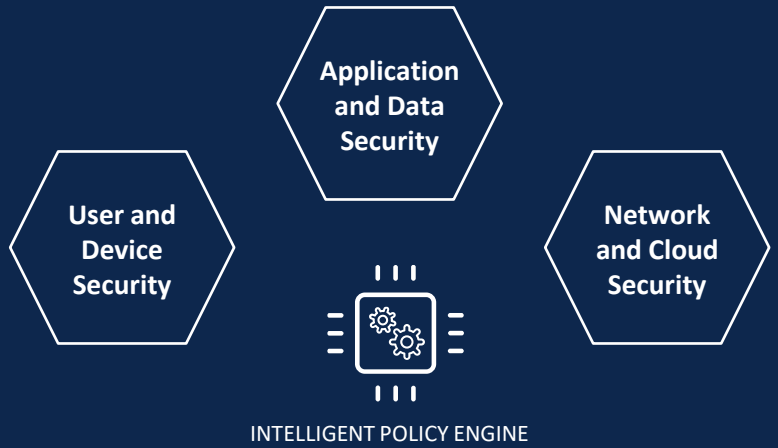
That are brought together and united



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Manage access with an app first approach

Independently and layered together



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero Trust Microsegmentation



What's Driving the Need for Microsegmentation?



Suffer from cyber fatigue (staying ahead of threats)[1]



Orchestration between products is challenging[1]



Network security at the edge is more difficult[2]



of CISOs find it very or extremely challenging to secure data in public cloud[3]

[1,2] Cisco CISO report 2020 [3] ESG cloud report 2020
[3] Cisco 2020 CISO Benchmark Report

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IT teams are struggling to keep up



of organizations want to release new changes weekly or more frequently and be able to restore service between one hour and one day…





of organizations cite manual processes and siloed teams as top bottlenecks in app delivery pipelines

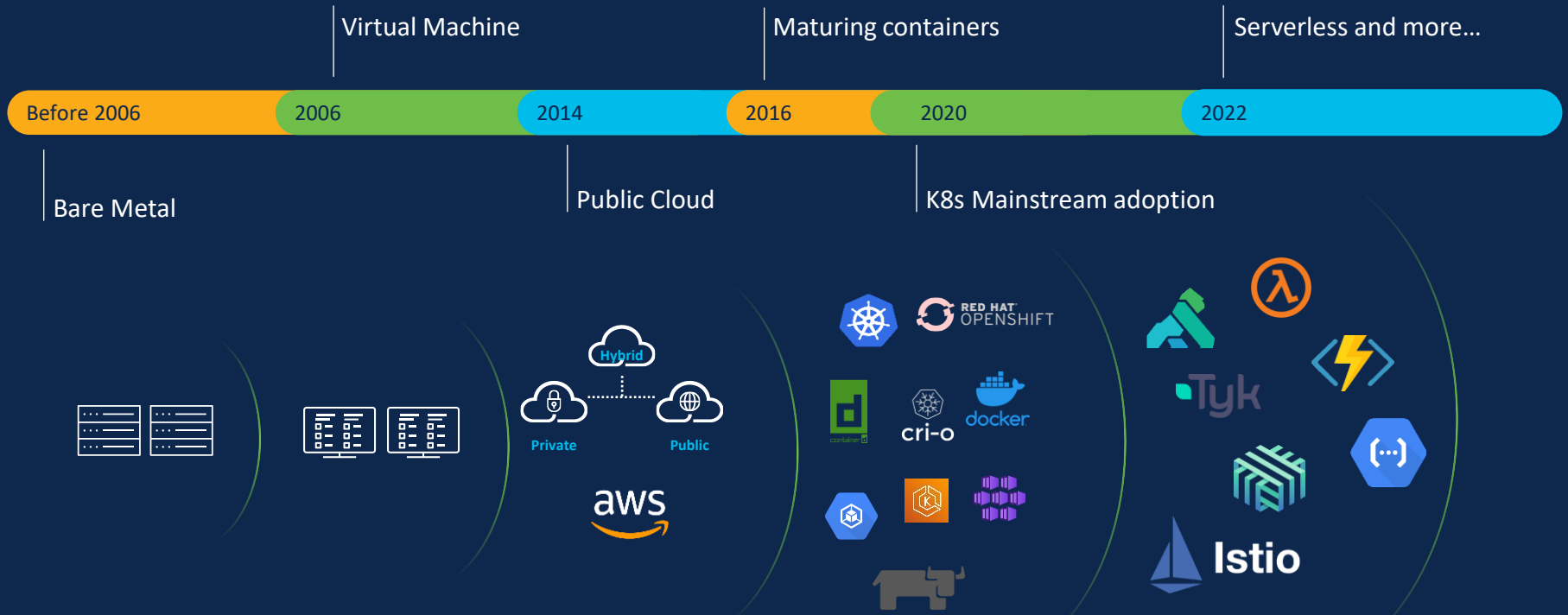
…but it can be challenging

- increasingly distributed environments
- complexity beyond human scale
- integrating with devops toolchains
- new and unfamiliar control points

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

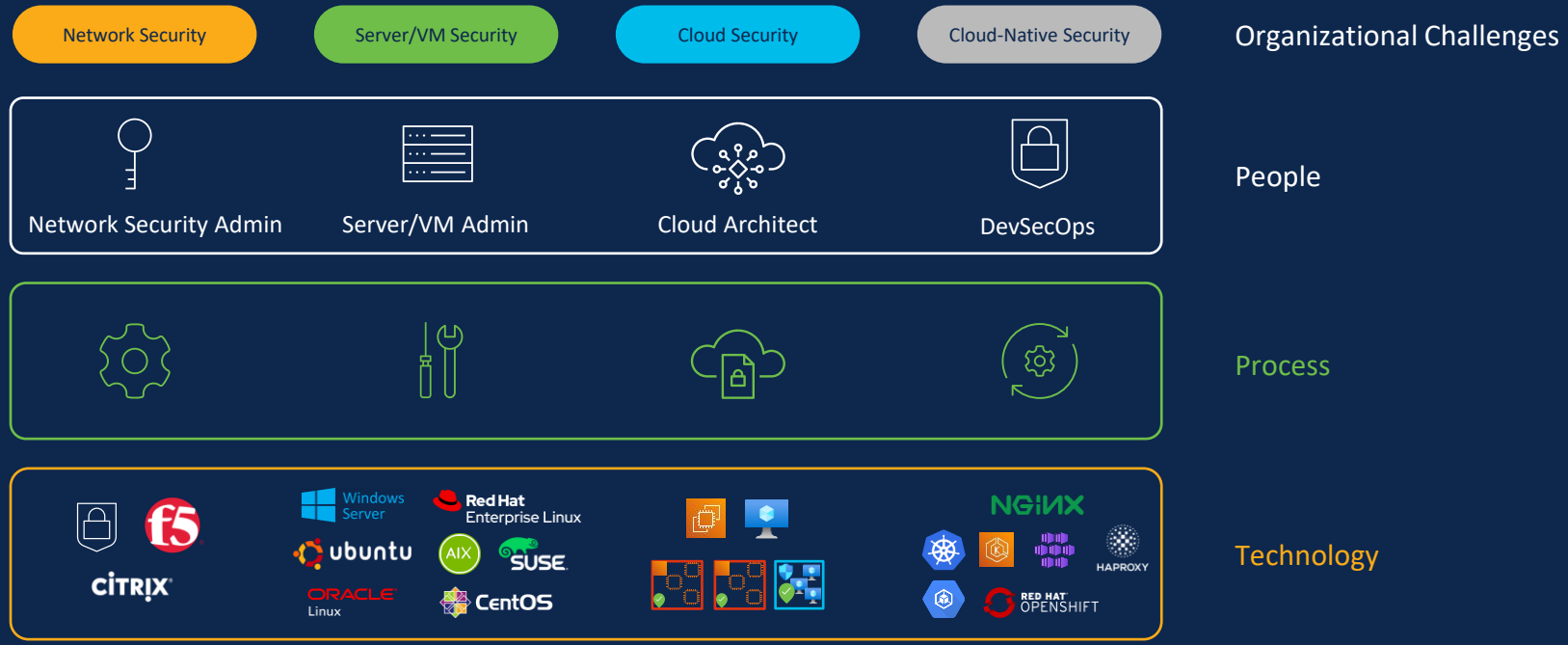
Sources: Google: State of DevOps 2019, IDC US, DevOps Survey 2019, July 2019

Technology evolution



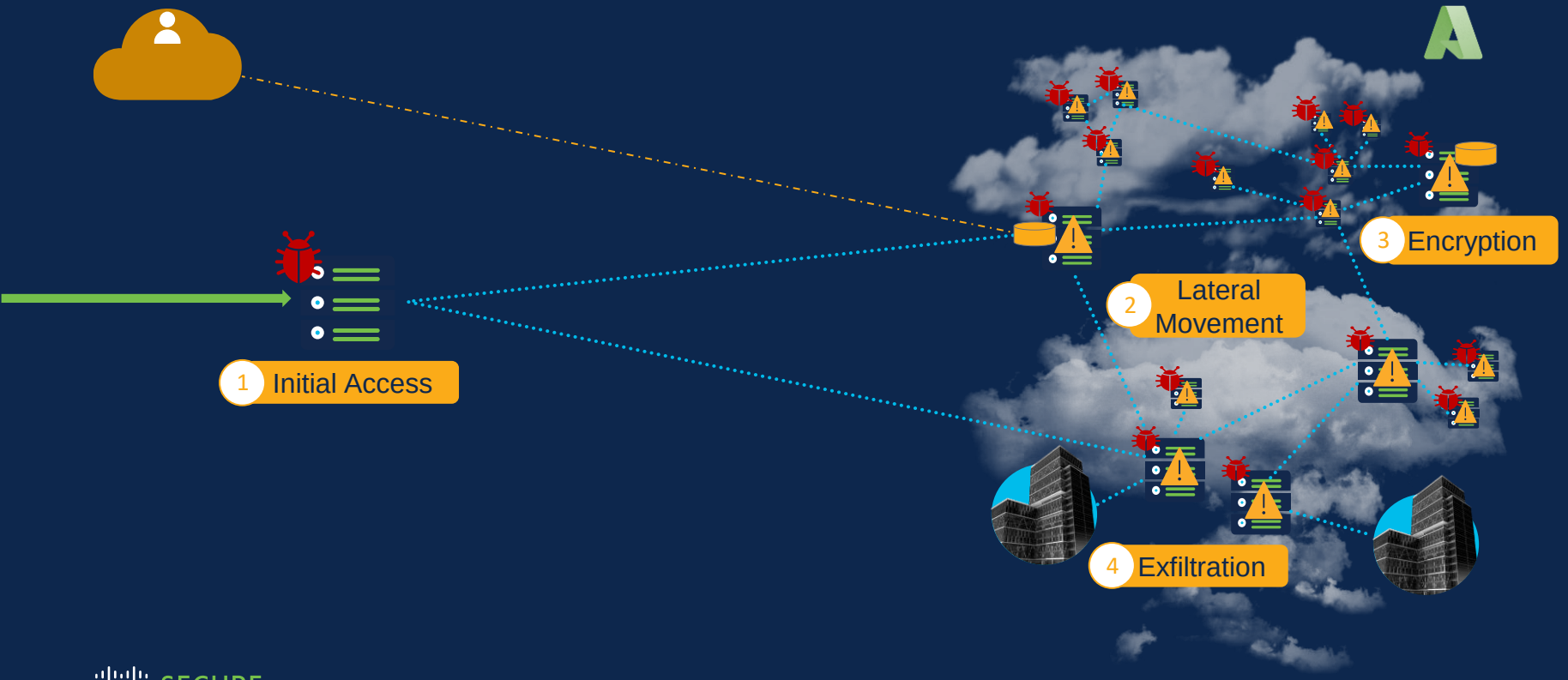
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Policy control and organizational challenges



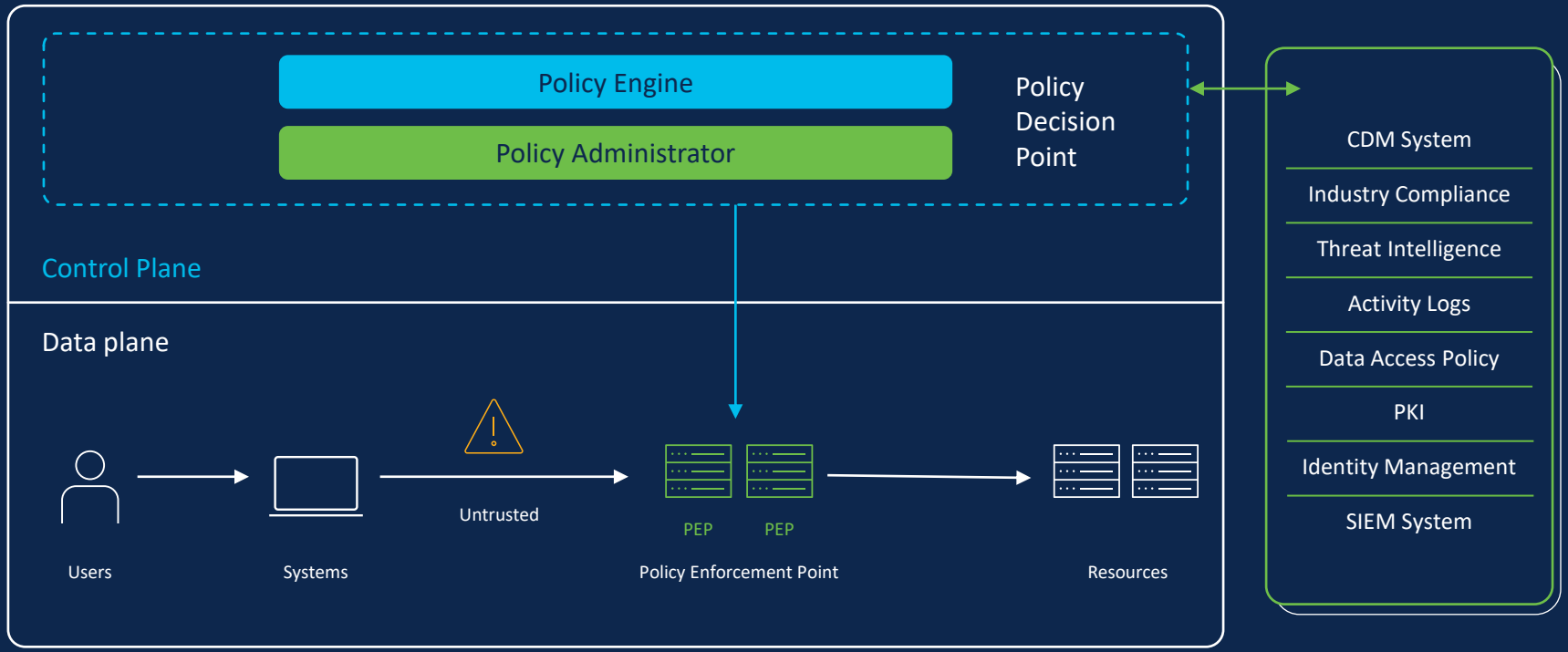
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Anatomy of a Breach



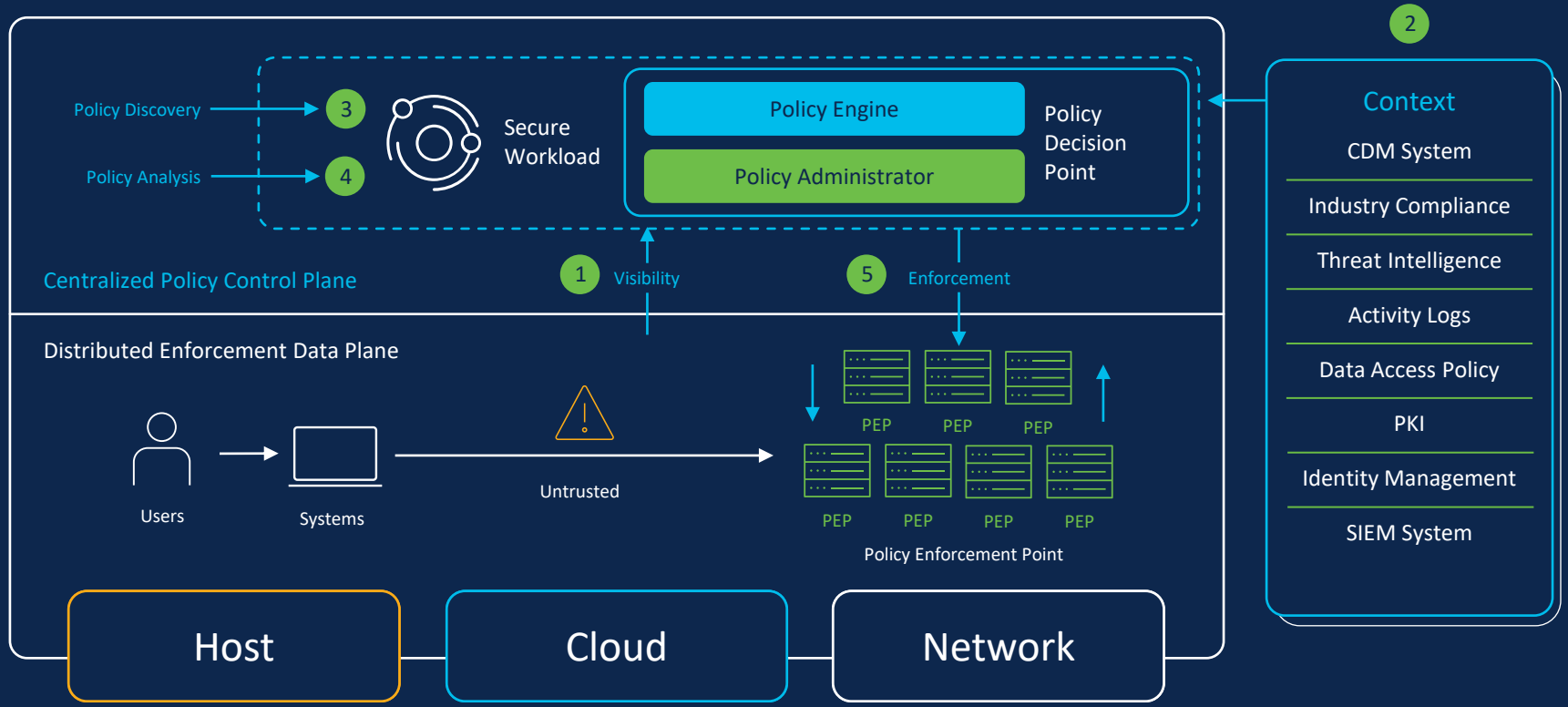
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

NIST 800-207 – Zero Trust Architecture



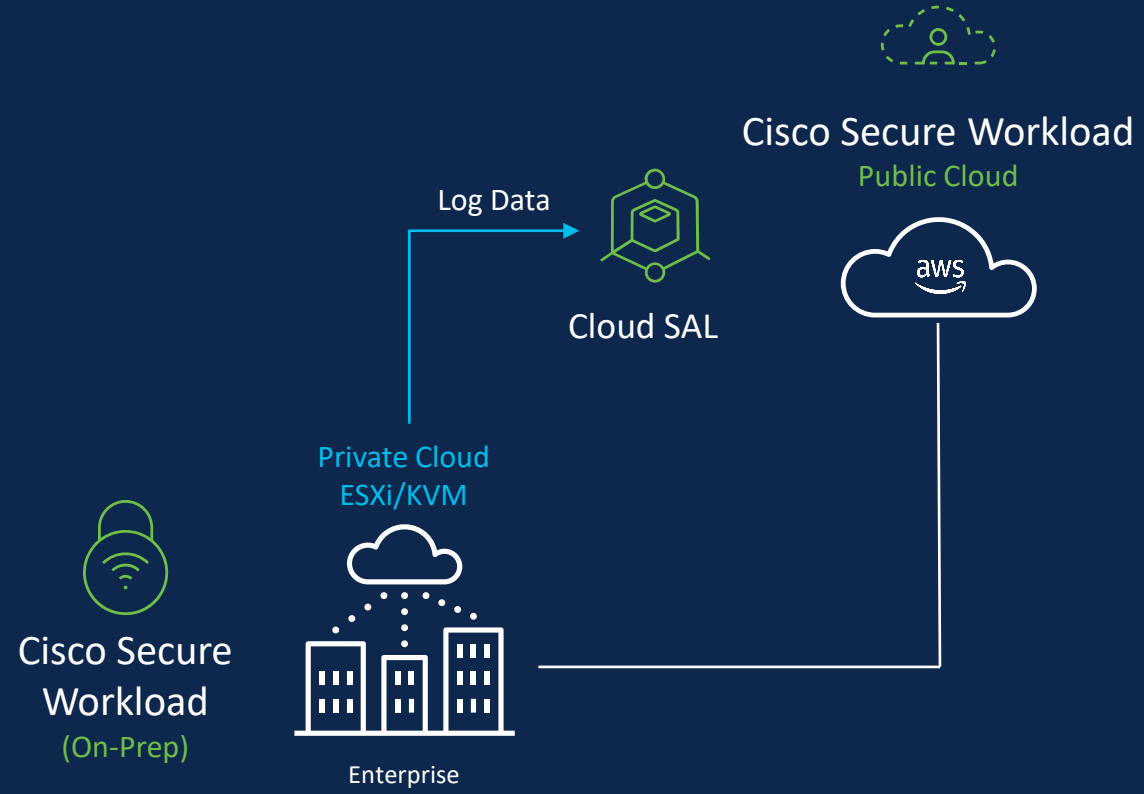
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Workload and NIST 800-207



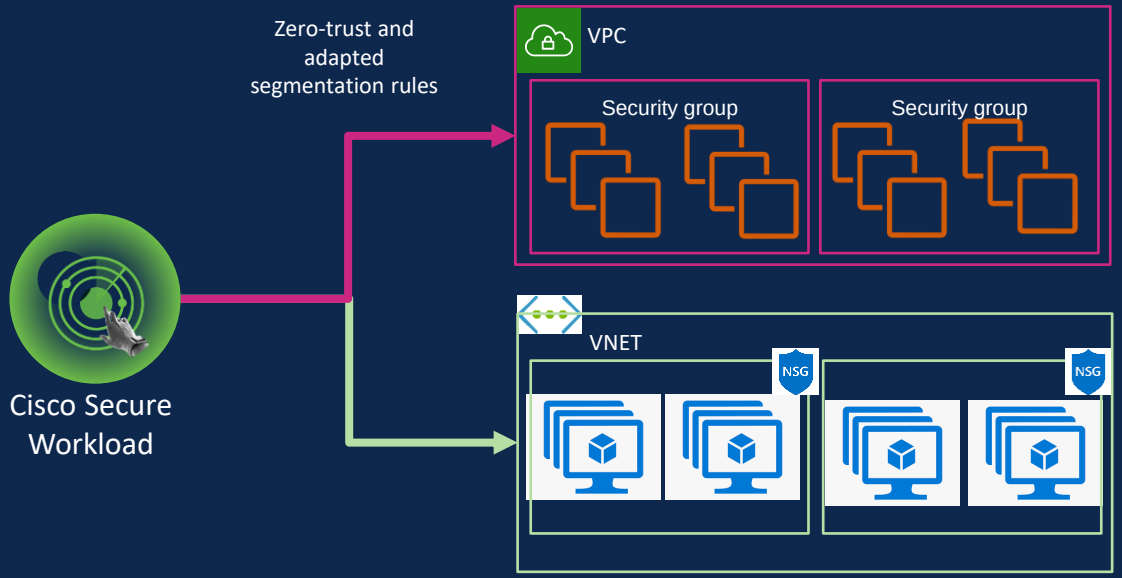
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Use Case - Securing Hybrid Environments



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Use Case – Securing Public Cloud workloads



Cloud onboarding and management workflow

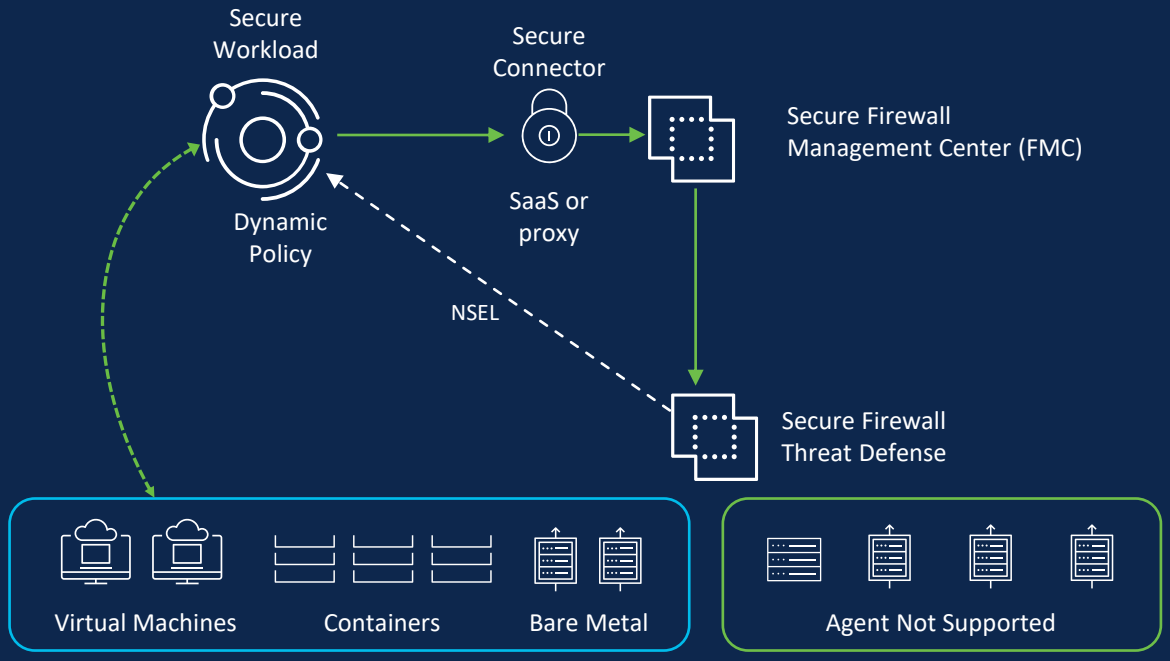
Unified configuration and management UI workflow for all public cloud capabilities

- Single onboarding wizard to enable cloud integration capabilities
- Provision to automate necessary roles and permission creation based on the selected capabilities
- Option to auto create scopes based on VPCs or VNETs as part of the workflow
- Single UI to monitor the status and details of all the enabled capabilities for cloud integration

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

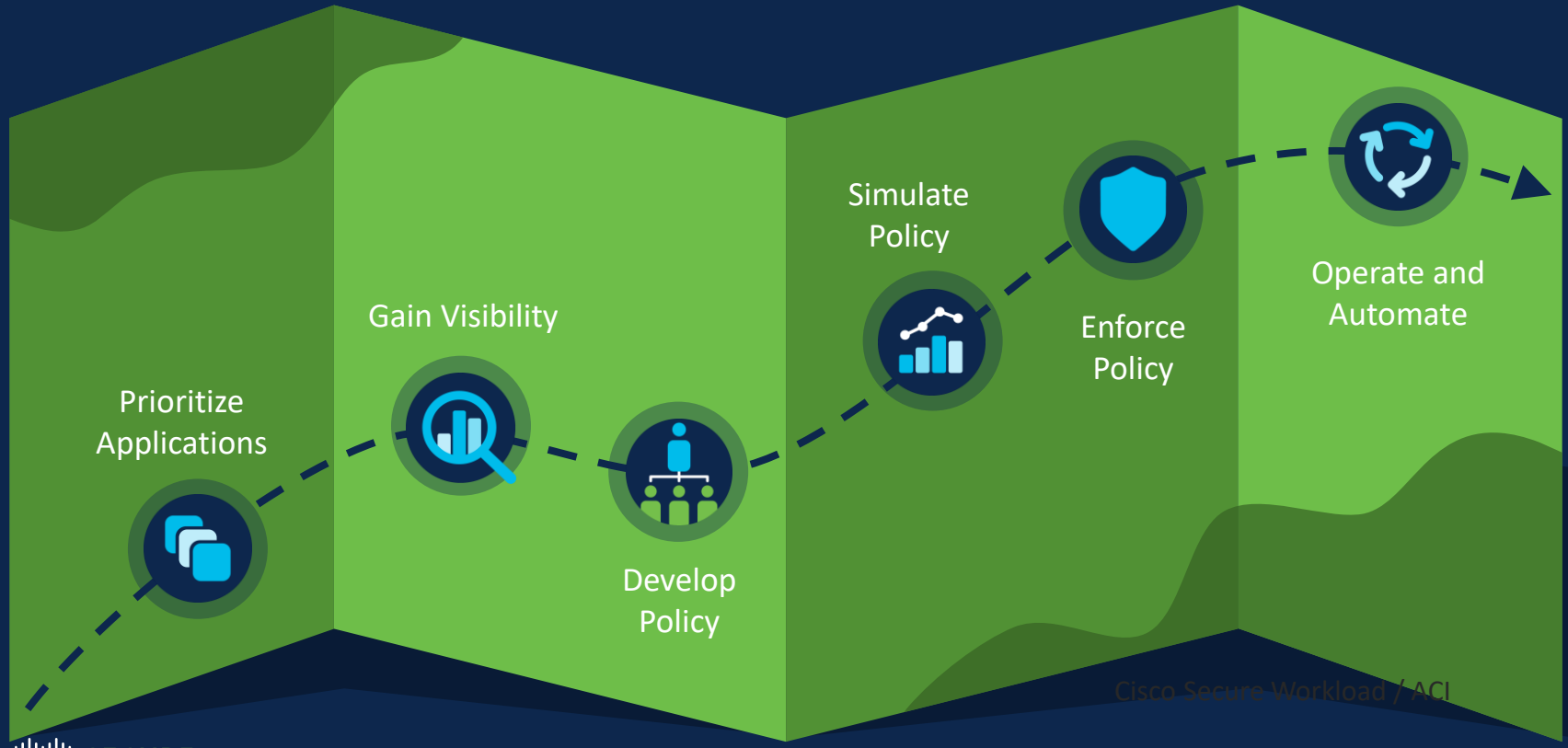
Secure Workload and Secure Firewall Integration

Use Case – Agent and Agentless protection



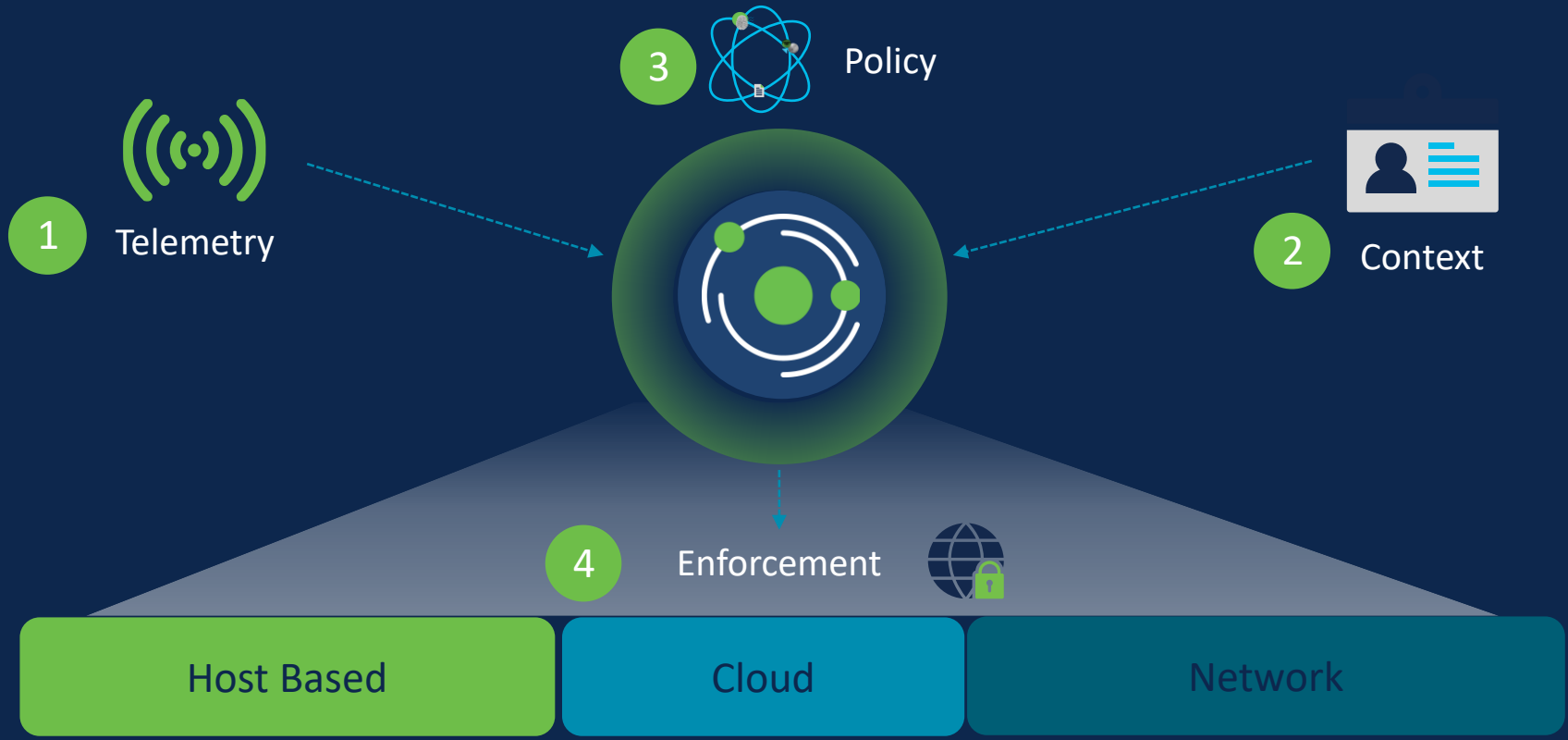
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Steps to Application Segmentation



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Workload in Nutshell



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

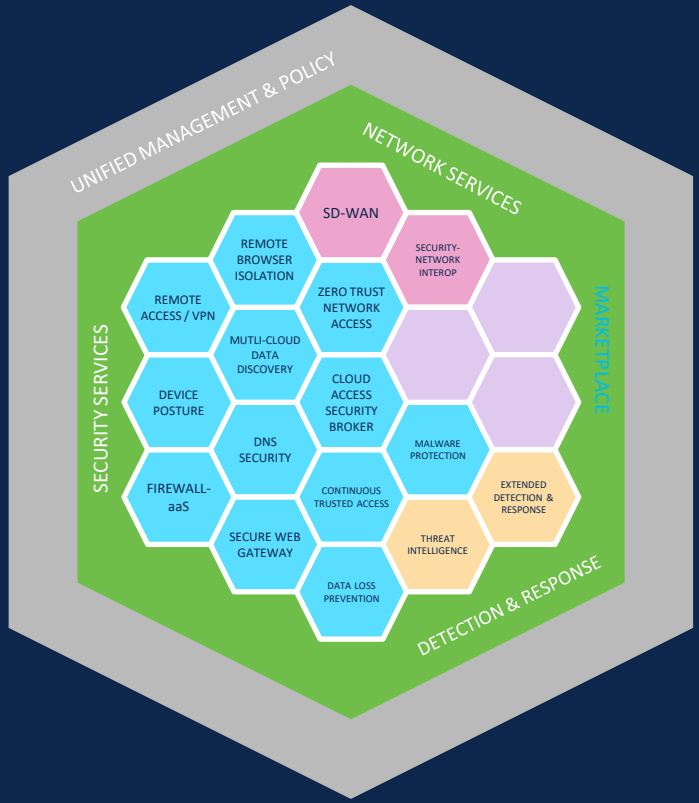
What about the User



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Unified Management & Policy

- Persona-driven management dashboards
- Configure many services simultaneously
- Automatically detect and resolve conflicts
- Leverage telemetry to define policies through intent or intelligence



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Unified Management & Policy

INTENT-BASED

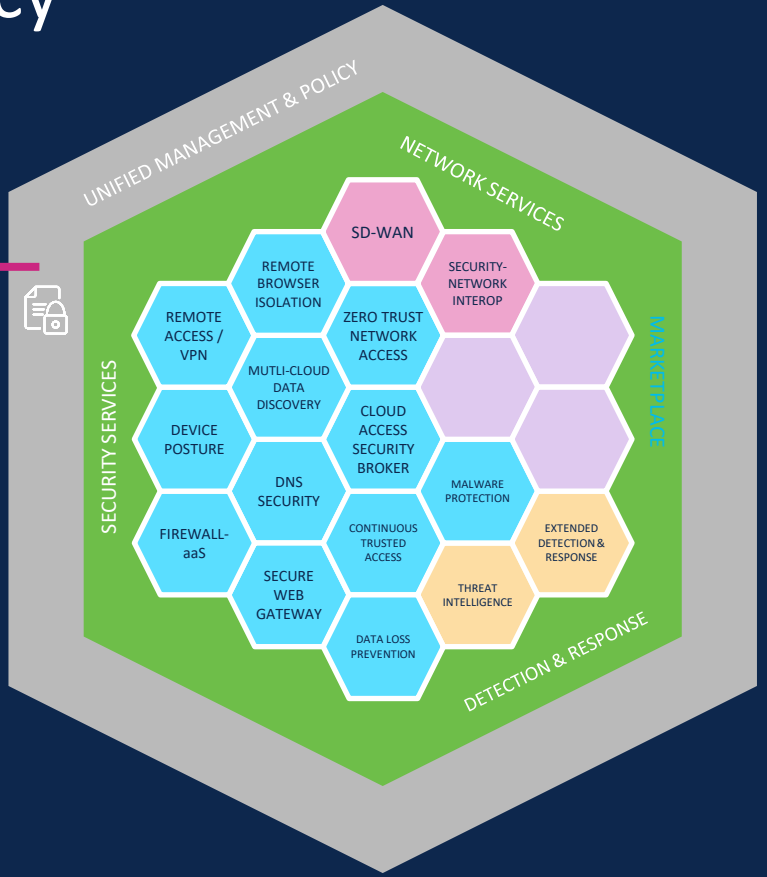


SECOPS ADMINISTRATOR

CREATE POLICY

"Allow Maria to access enterprise applications like Salesforce and Gainsight from her work Mac and iPad if she is accessing them from the United States.

She should be allowed access to personal financial systems such as her Coinbase account, but with a Browser Isolation instance so that no malware from these sites infects her computer."



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Unified Management & Policy

INTENT-BASED



SECOPS ADMINISTRATOR

CREATE POLICY

"Allow Maria to access enterprise applications like Salesforce and Gainsight from her work Mac and iPad if she is accessing them from the United States.

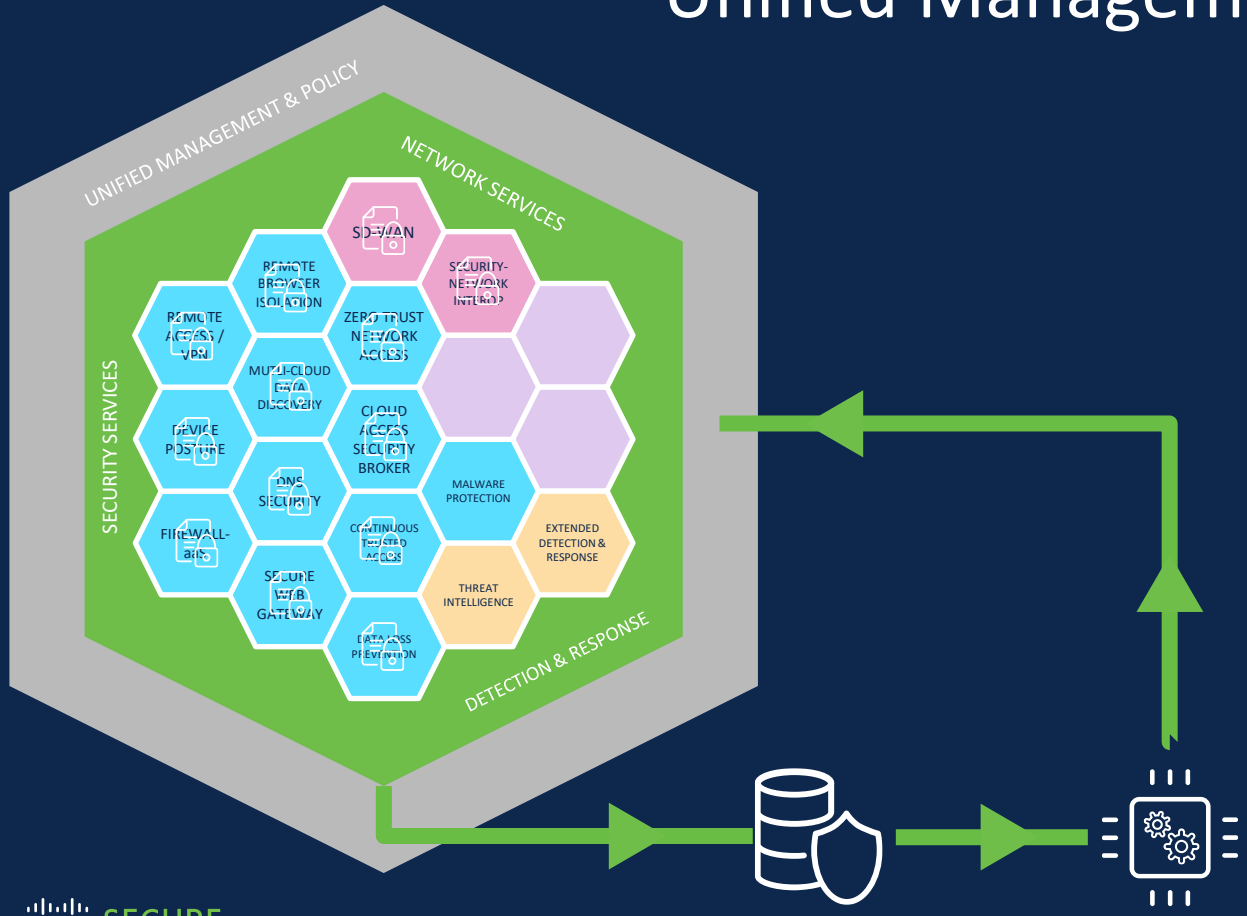
She should be allowed access to personal financial systems such as her Coinbase account, but with a Browser Isolation instance so that no malware from these sites infects her computer."



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Unified Management & Policy

INTELLIGENCE-BASED



AUTOMATED

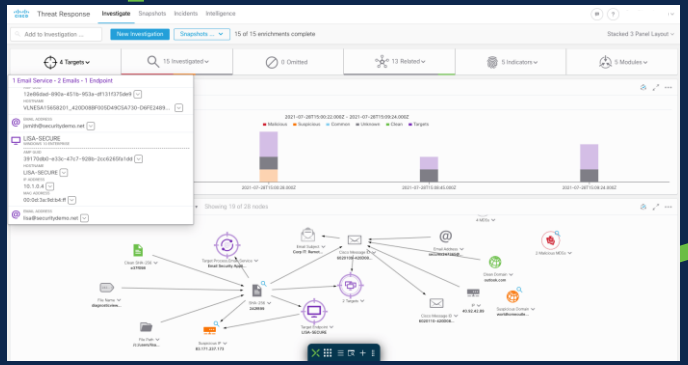
Use intelligence technology to analyze data collected from endpoint agents, and all aspects of the security cloud infrastructure and services, to create policies automatically. This approach can react faster and find threats that may not be obvious to human SecOps personnel.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threat Intelligence, Detection & Response

SECOPS ADMINISTRATOR

AI-BASED RESPONSE ENGINE



CLOUD ACCESS SECURITY BROKER

MUTLI-CLOUD DATA DISCOVERY

REMOTE BROWSER ISOLATION

REMOTE ACCESS / VPN

SD-WAN

EMAIL SECURITY

WEB APPLICATION FIREWALL

THREAT INTELLIGENCE

FIREWALL-aaS

DDoS

EXTENDED DETECTION & RESPONSE

SECURE WEB GATEWAY

CONTENT DELIVERY NETWORK

DNS SECURITY

MALWARE PROTECTION

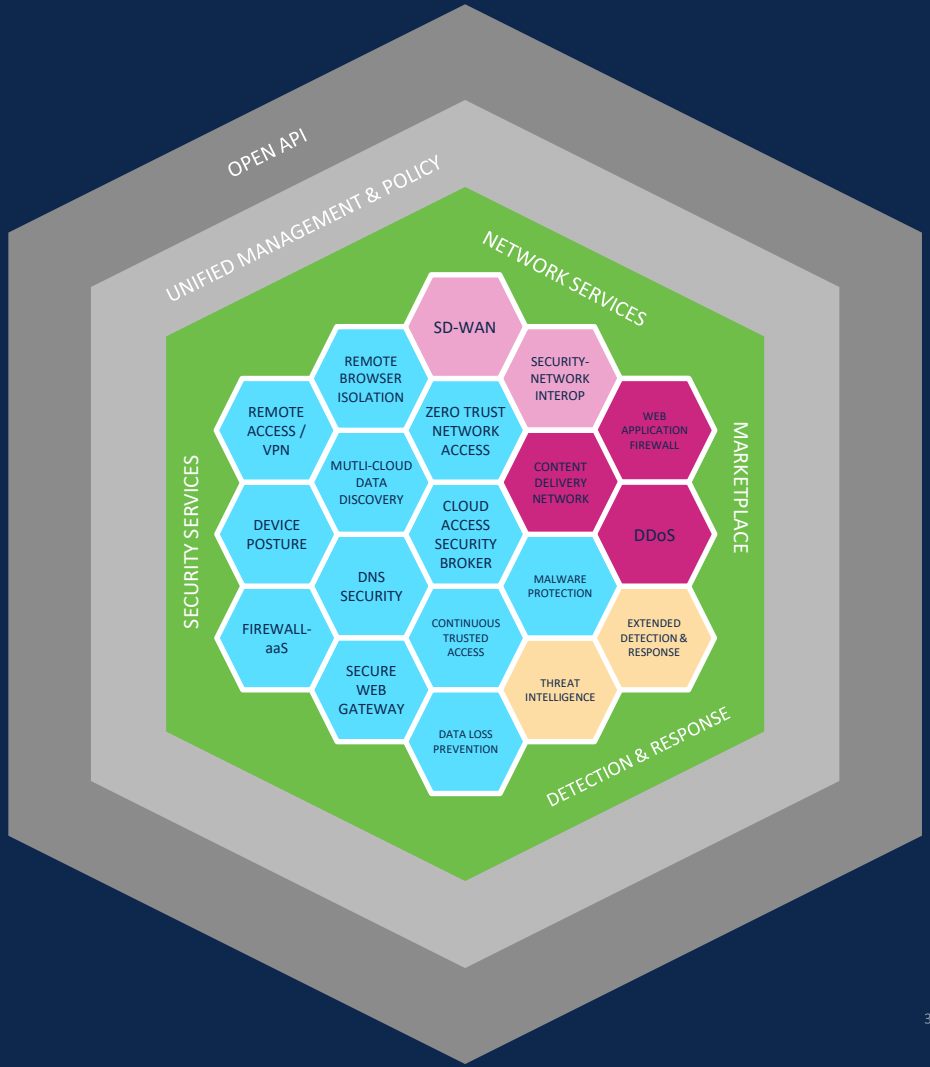
CONTINUOUS TRUSTED ACCESS

DATA LOSS PREVENTION

ZERO TRUST NETWORK ACCESS

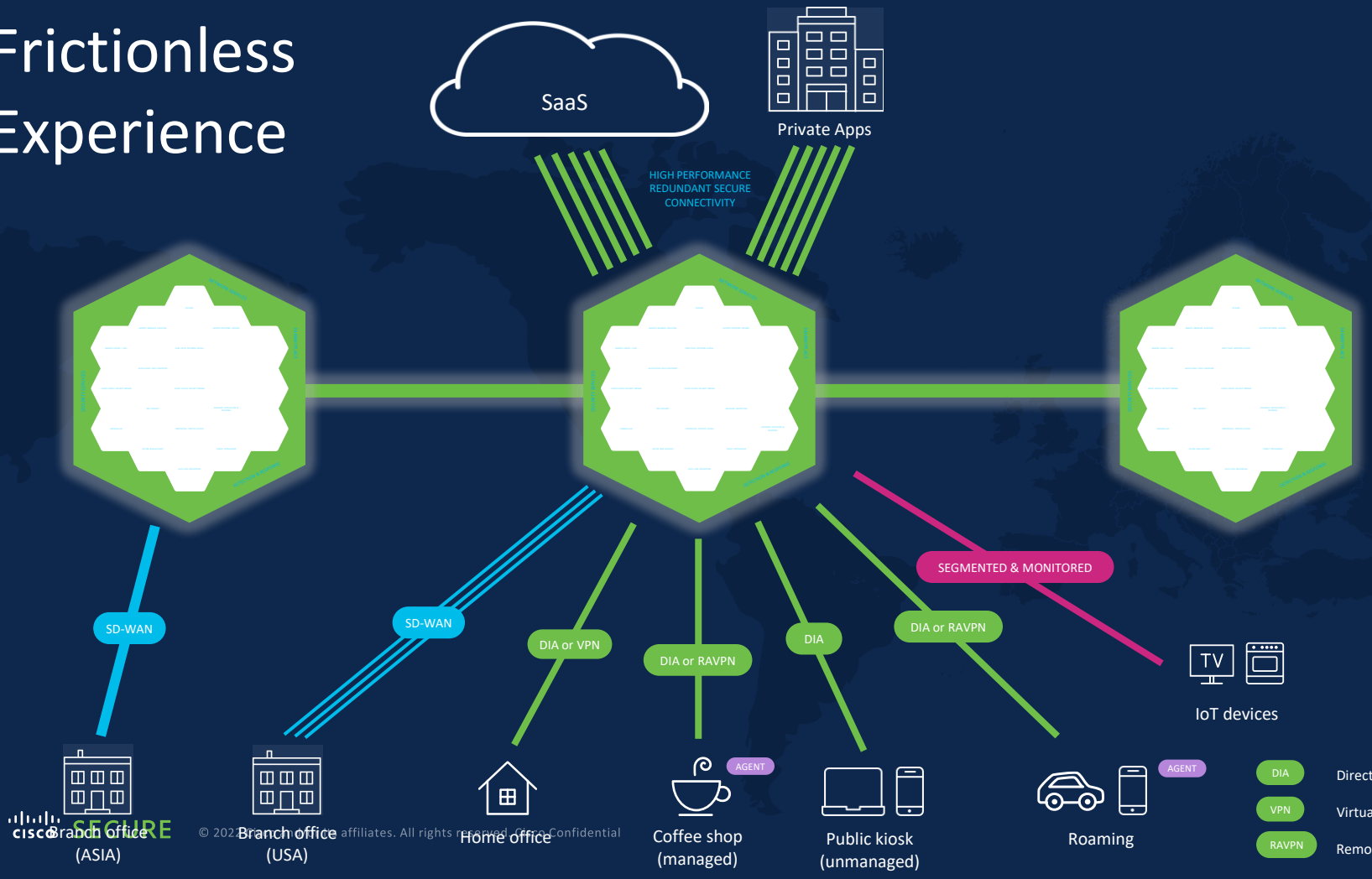
Open API

- Connect southbound to any IaaS
- Connect northbound to any PaaS
- Provide extensibility with third-party ISVs



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Frictionless Experience



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco and AWS innovate to make operations easier

Centralizing cloud governance in one click with AWS Control Tower



Save time when deploying security and networking infrastructure in AWS

Cisco-approved template-based design guides offered as products in AWS Service Catalog help you save time and reduce risk.



Simplify policy management with automation

Automatically establish AWS accounts and implement guardrails across your global AWS account list as environments change.



Maintain visibility across your multi-account AWS environment

Maintain compliance and governance in a single dashboard with visibility into AWS user accounts and audit accounts against enabled guardrails.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Thank you!

Justin Buchanan

Twitter: @JustnBuchnn



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

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