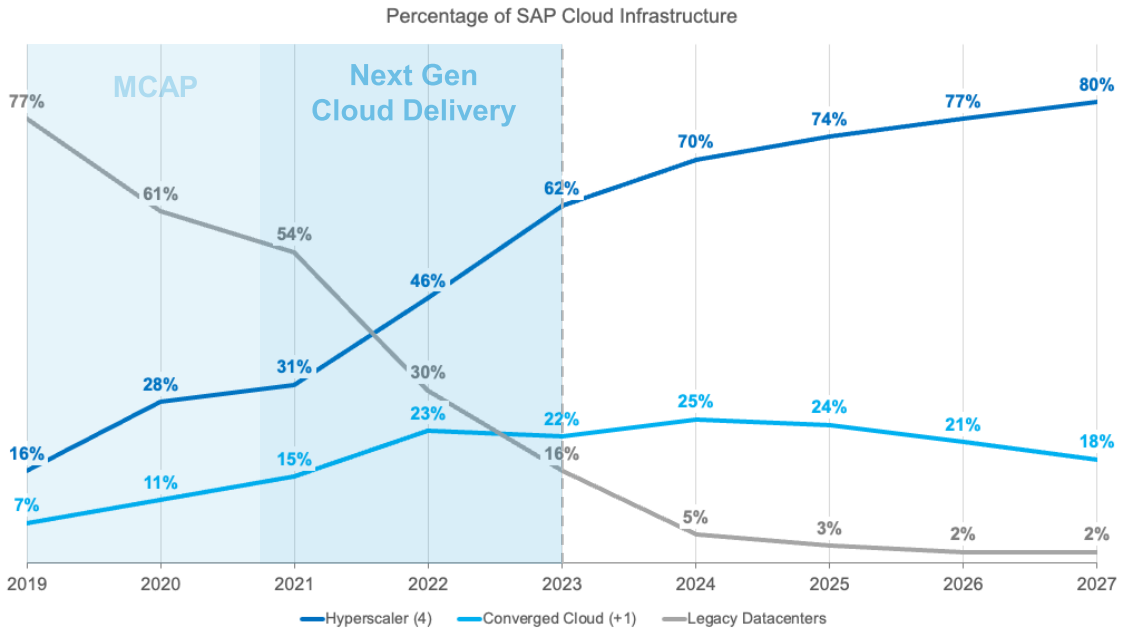
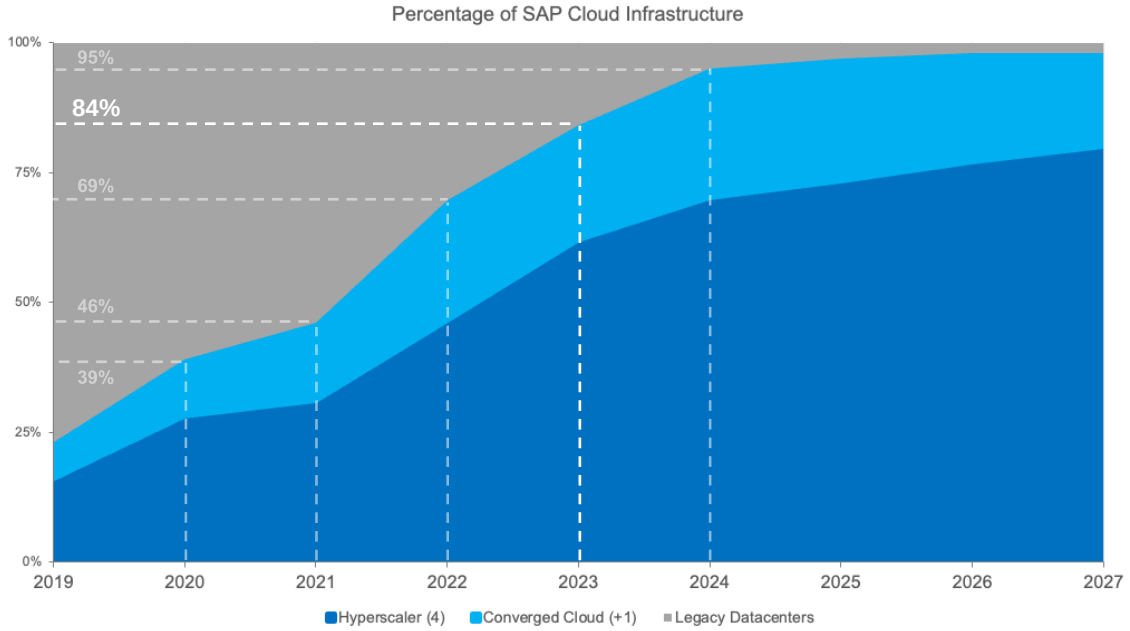
Masterclass: DevSecOps, SecDevOps and Secure Cloud Transformation Accountability through Cloud Security Engineering

Jay Thoden van Velzen
Strategic Advisor to the CSO, SAP

Rapid Cloud Transformation

Next-Generation Cloud Delivery Changed the Landscape





Rapid Cloud Migration

- Traditional data center landscapes dropped from over half of the environment to just a sixth, and projected to be just 5% by the end of 2023
- Public cloud grew to nearly two-thirds of the landscape through organic growth and cloud migrations

Accelerated Cloud Transformation

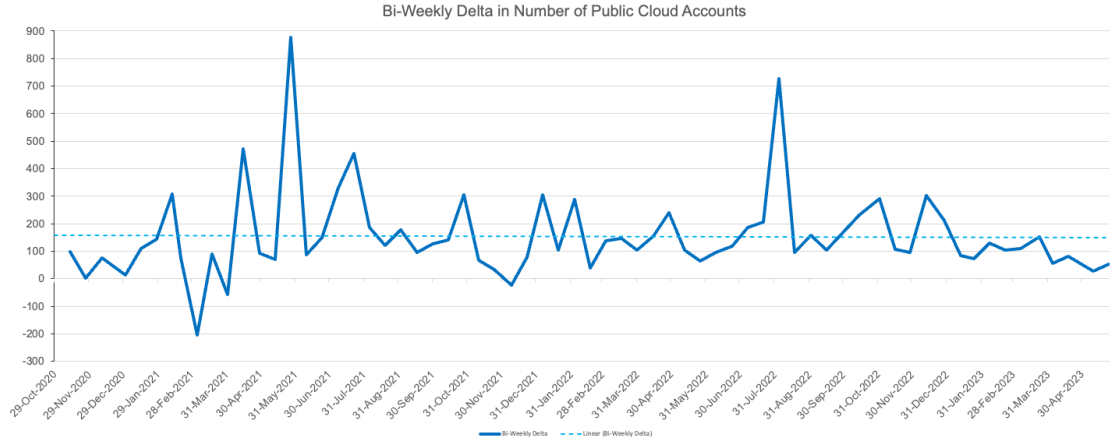
- At 84% of the landscape and 95% by end of 2023, the key security focus must be to protect SAP's cloud landscape
- Bringing our customers along

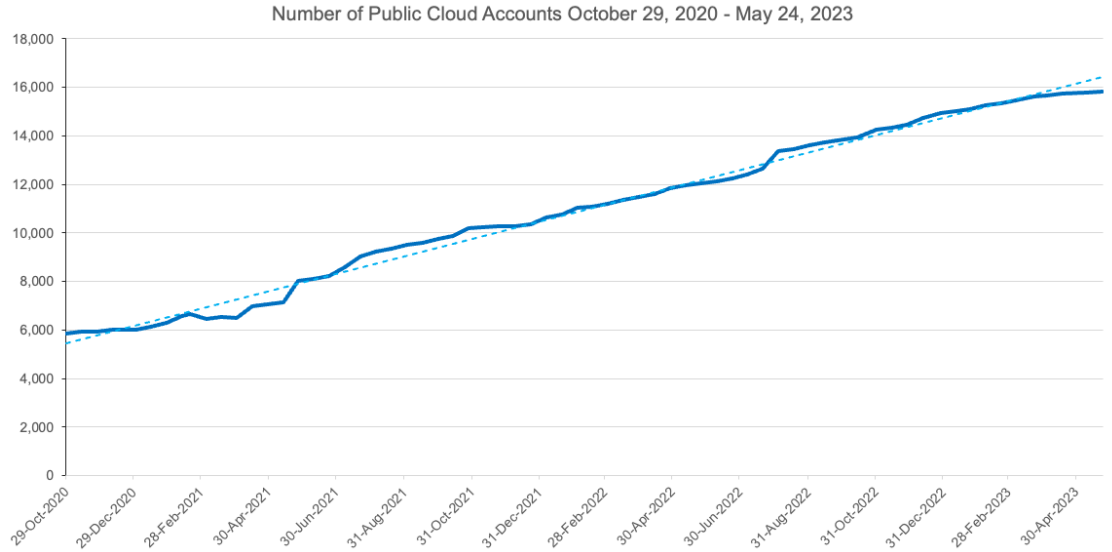
SAP's Public Cloud Use: A Sense of Scale and Responsibility

Unique Scale, Growth Rate and Multicloud

- Growth from 5,842 public cloud accounts at the start of Next Gen Cloud Delivery to 14,954 (+9,112) at the start of 2023 (+156%)
- ~15,900 today – 76.5% Production workloads
- SAP 2nd fastest growing cloud provider in Q2 (34%), Q3 (38%) and Q4 2022 (33%), and joint-3rd in Q1 2023 (24%) while uniquely Multicloud in the Top 10

- Source: AccelerationEconomy.com Cloud Wars





With Growth Comes Increasing Responsibility

- Corporate strategy projects this growth is set to continue for the foreseeable future
- Particularly sensitive and critical workloads

Large and Complex Organization

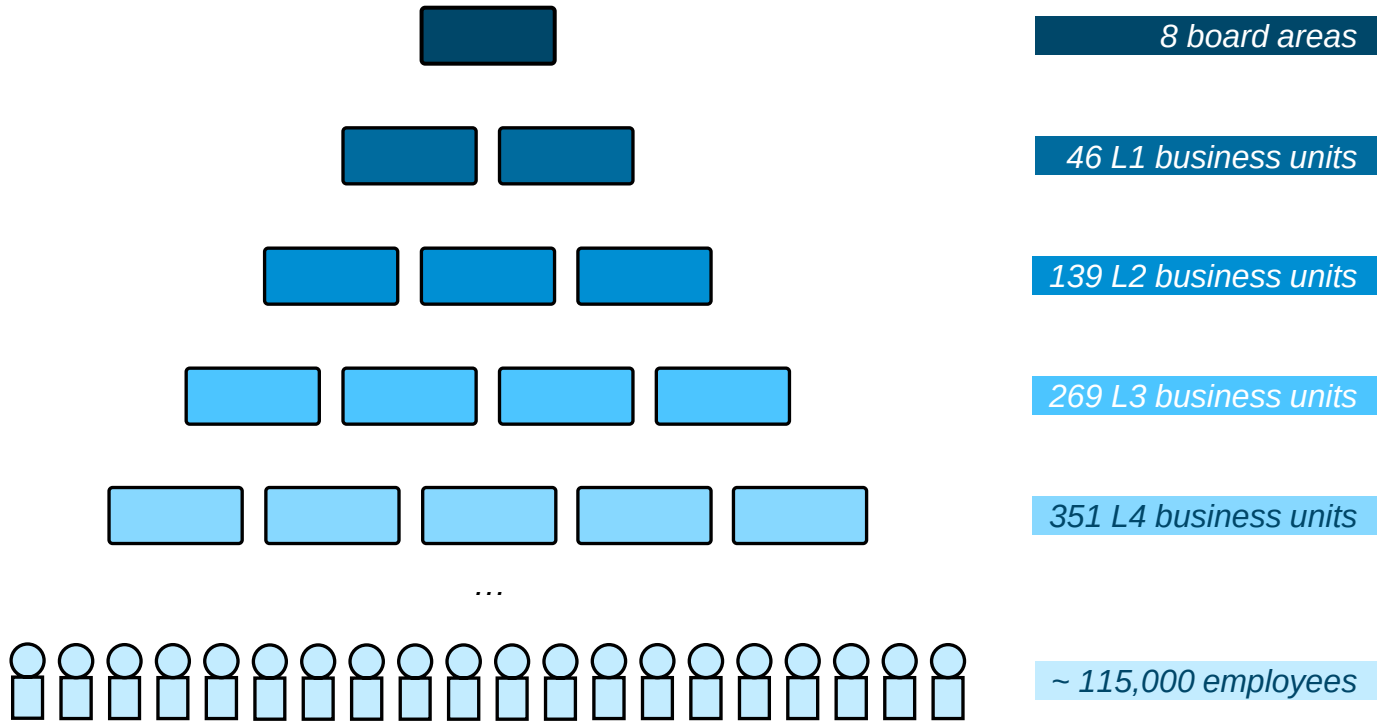
Multi-layered

- 6-8 levels of organizational hierarchy by cost center
- Organizational change happens regularly, as well as changes in the workforce

Pervasive Cloud Use

- Product (58%) and Platform (37%) board areas dominate cloud account use, but still leaves 5% (~750) for internal IT, SGS, Customer Success, People Operations, Marketing & Solutions and GF&A
- Variety of resources, cloud maturity, and skill level

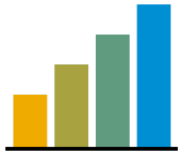
Teams operating active cloud accounts



Cloud Challenges

Scale

- This size becomes very abstract
  - – You can’t walk through a data center to get a sense
- Even small mistakes get amplified quickly
- Every manual process breaks



Growth During Transformation

- There is no time – growth drives its own momentum
  - – Delay makes any problem bigger
- Organizational change is hard
  - – Even more for non-tech teams!

Level of Complexity

- Multicloud by strategy
- Large portfolio of products, often deployed in regulated industries
- Transitioning to cloud-native and micro-service architectures
- Bewildering organization with high autonomy within business units and developer teams

Cloud Security Challenges

Scale

- Large scale means many findings (good or bad) – everything is an engineering job
- Everything can break at any time, no “test” environment

Growth During Transformation

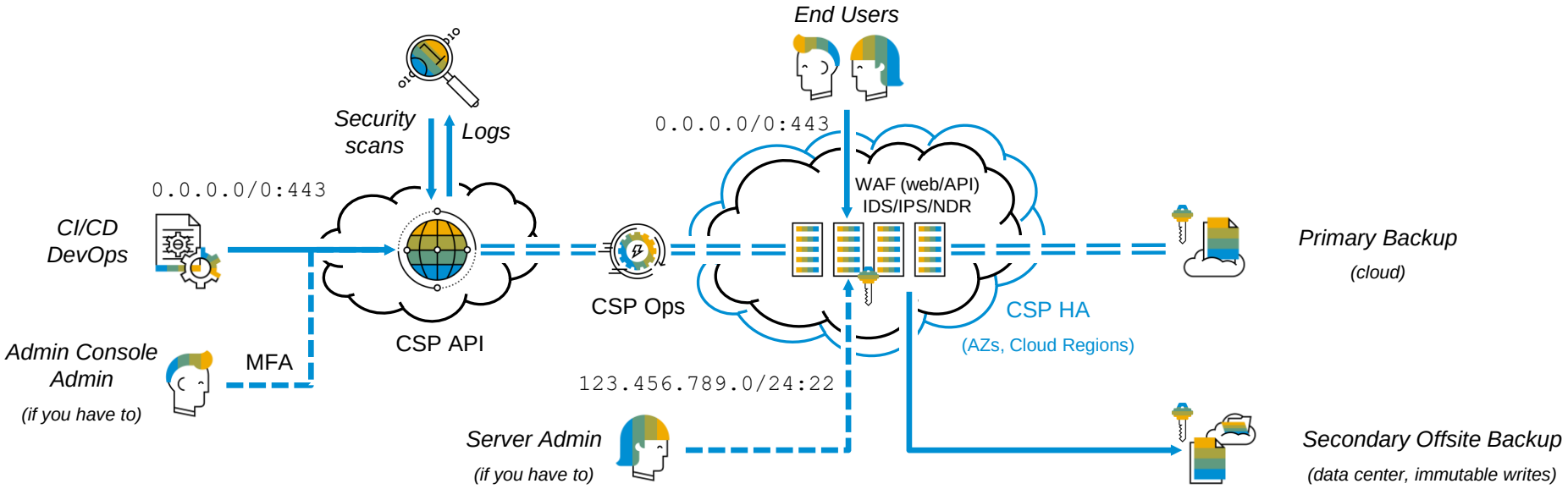
- Our security budget doesn’t grow linearly with growth in the landscape – does yours?
- Security organizations often don’t run or adapt to change as fast as DevOps teams

Level of Complexity

- How do you centralize security functions when developer teams have even more autonomy?
- How do you make them not hate you, for making them do work to get more work?
- How do you get access to systems or get tooling deployed?

Security and Administration – Cloud Focus

Infrastructure-as-Code, Out-of-Band Administration, High Availability, Secure Backups



API-based Administration and Monitoring

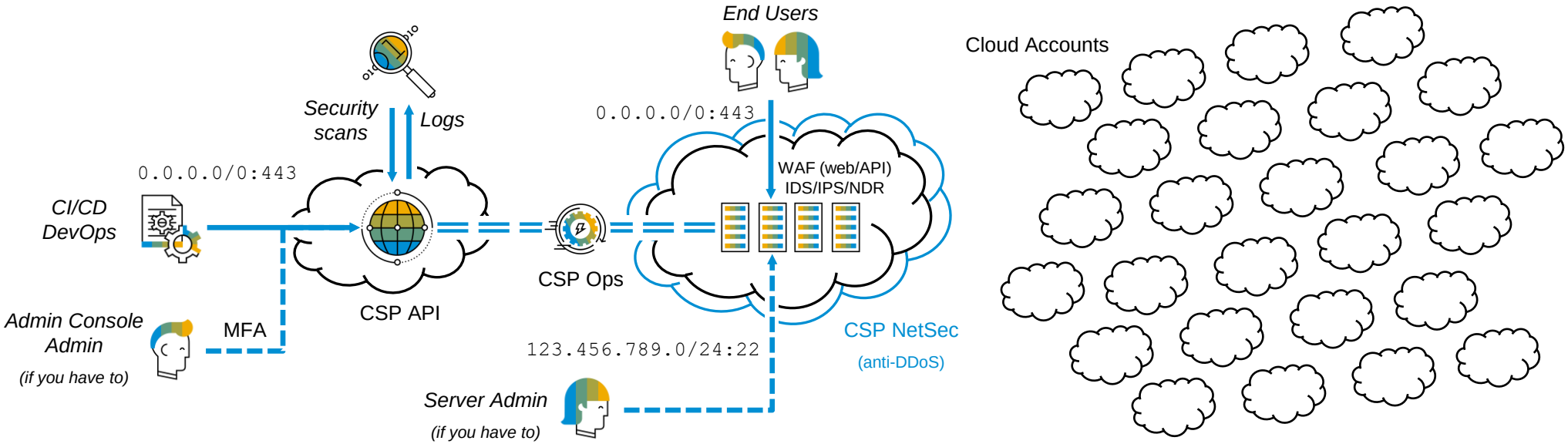
- Deployments typically through CI/CD pipelines and DevOps – we discourage the use of web admin console
- Direct SSH server administration discouraged – if inevitable must be via approved CIDR ranges
- (Most) security scans and log collection via cloud API and cloud organizational policy controls

Resiliency

- Built-in cloud resiliency capabilities (AZs, Multi-Region)
- Primary and secondary (offline immutable) backup
- Enforced encryption standards
- Restoration of landscapes by restoring backups and redeploying landscape – if needed

Security and Administration – Cloud Focus

Out-of-Band Administration at Mass Scale and Tenant Isolation



API-based Administration and Monitoring

- Deployments typically through CI/CD pipelines and DevOps – we discourage the use of web admin console
- Direct SSH server administration discouraged – if inevitable must be via approved CIDR ranges
- (Most) security scans and log collection via cloud API and cloud organizational policy controls

Separate Isolated Islands

- Different cloud accounts for different purposes are not connected unless explicitly required, reducing blast radius dramatically
- Utilizes cloud providers' built-in tenant isolation
- Many SAP solutions single-tenant deployed
  - A bit more complicated for multi-tenant solutions but general principle holds

Cloud Security Posture Management

inside the VM

inside the container

own-run Kubernetes

own-run serverless

CIEM

attack paths

on disk

PII/DPSM

own-run databases

- Started with CSPM in 2018
- Tracking and enforcement since 2019
- 95% reduction of high severity misconfigurations in 2020
- Home-grown solution deployed 2022
- ~99% compliance rate

cloud API

IAM

public/private

encryption, secrets, keys

managed Kubernetes (EKS)

managed databases

network configuration

compute (EC2)

block storage (EBS)

object storage (S3)

Cloud Service Configuration

Leverage the IaaS Providers' Organizational Policy Engines

Cloud Defender Techniques via Cloud API and Organizational Roles

General Administration

- Forcing all cloud accounts into organizations enables powerful defensive capabilities and controls to make them behave more secure-by-default

- All accounts in SAP cloud provider organization
- Enforce password policy
- Enforce MFA for cloud admins

Logging

- Centrally enforced logging that cannot be removed ensures a direct event ingestion into SIEM that attackers can neither see nor manipulate

- API/Audit and storage access logging applied and cannot be de-activated
- Logs centrally collected and ingested into SIEM

Internet-Facing/Publicly Accessible

- Protects against common cloud network misconfigurations of unintentionally publicly accessible resources

- Enforce block-listed ports not exposed to internet
- No block storage, storage buckets or snapshots public

Encryption

- Enforcing encryption-at-rest and in-transit standards, and secure key and secrets management

- Enforce TLS 1.2+
- Encryption enforced on block storage and storage buckets
- Enforce secure KMS/Key Vault config

Version 1 – 4 of Cloud Asset Management Attribution

Who Owns What So We Can Direct Alerts to the Appropriate Team

This proved very useful later!

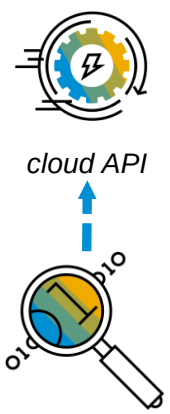
	Improvement	*Reason*
Version 1 2017	▪ Account owner, Cost Center Owner and Cost Object on account creation ▪ Allows assignment to org hierarchy	▪ Assigns who pays and who is responsible for administration ▪ Forced all accounts into SAP orgs
Version 2 Sep 2020	▪ Established mandatory periodic updates of metadata and new tags ▪ Non-compliance can lead to account locking, and even deletion	▪ Version 1 was optimized for growth, not full lifecycle management ▪ Out-of-date metadata complicated assignment and tracking
Version 3 Oct 2022	▪ Resource asset management (rather than cloud account) for more fine-grained alert and incident assignment	▪ Multiple resources deployed by different teams in the same cloud account; redistribution of findings ▪ Delays in remediation, added admin
Version 4 TBD	▪ Refocusing towards a release-based rather than asset-based approach to ensure shortest path to those who can remediate any finding	▪ Who owns the release and last touched a configuration matters more than who owns the asset

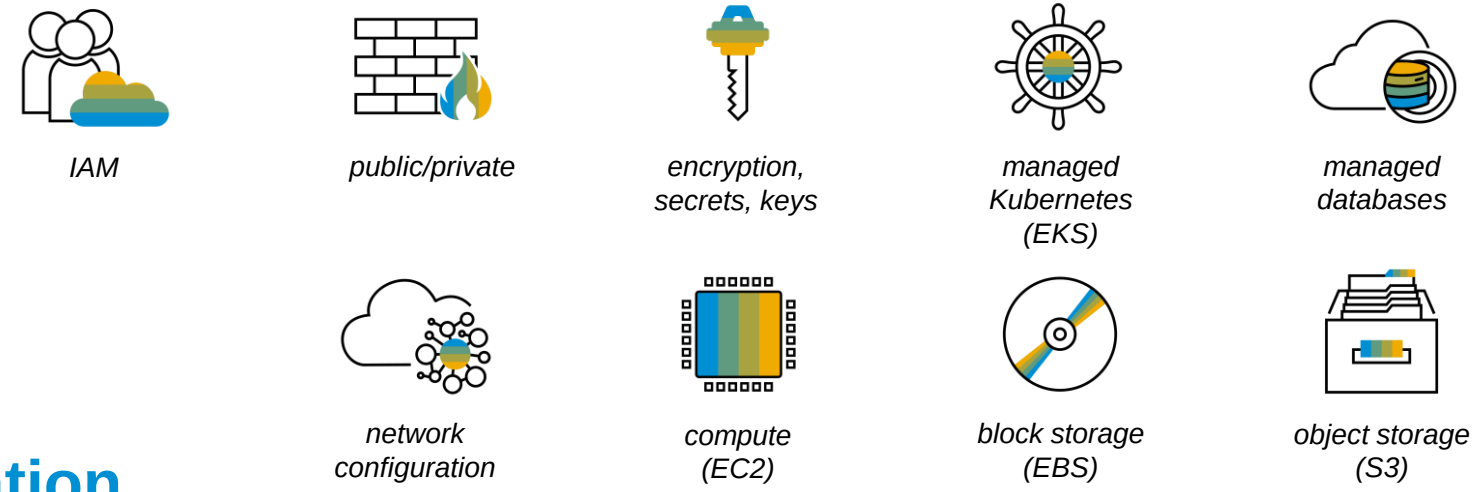
Visibility Higher Up the Stack?

How visibility higher up?

- Agent-based solutions, requiring developer effort
- Not very cloud-native, data center tooling
- Run and operating costs
- Slow onboarding process
- Tool sprawl

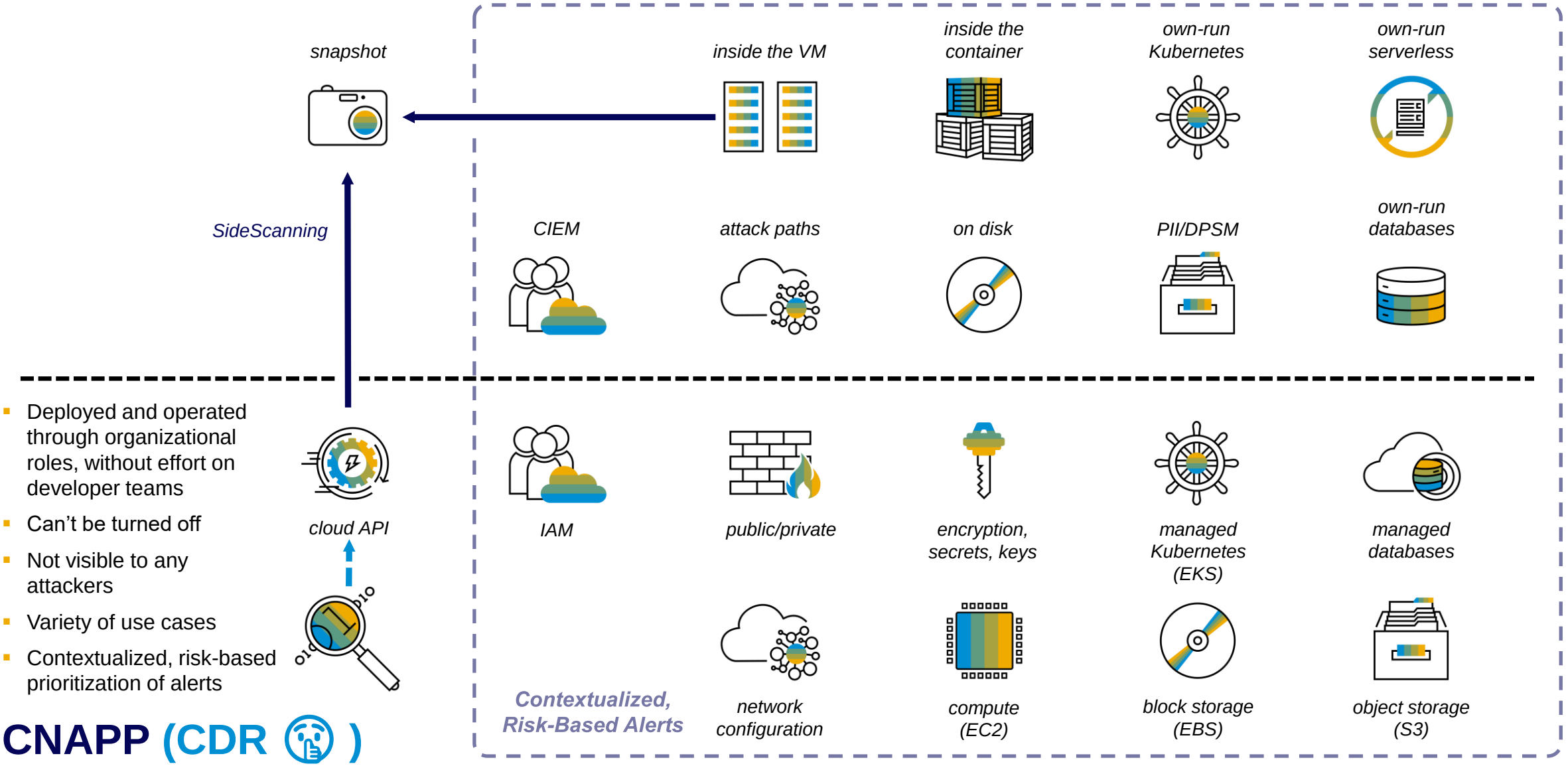
- Started with CSPM in 2018
- Tracking and enforcement since 2019
- 95% reduction of high severity misconfigurations in 2020
- Home-grown solution deployed 2022
- ~99% compliance rate





Cloud Service Configuration

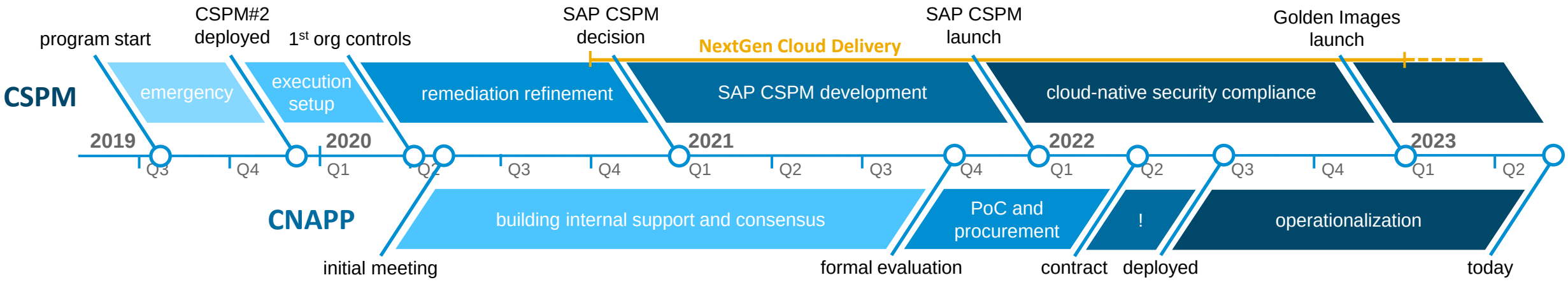
Visibility Higher Up the Stack



- Deployed and operated through organizational roles, without effort on developer teams
- Can't be turned off
- Not visible to any attackers
- Variety of use cases
- Contextualized, risk-based prioritization of alerts

CNAPP (CDR)

SAP Public Cloud Security Timeline



Cloud Security Posture Management

- Remediation of cloud security misconfigurations for those already in public cloud
- 96% reduction in 2020, despite doubling cloud resources
- Commercial solutions faltering

NextGen Cloud Delivery

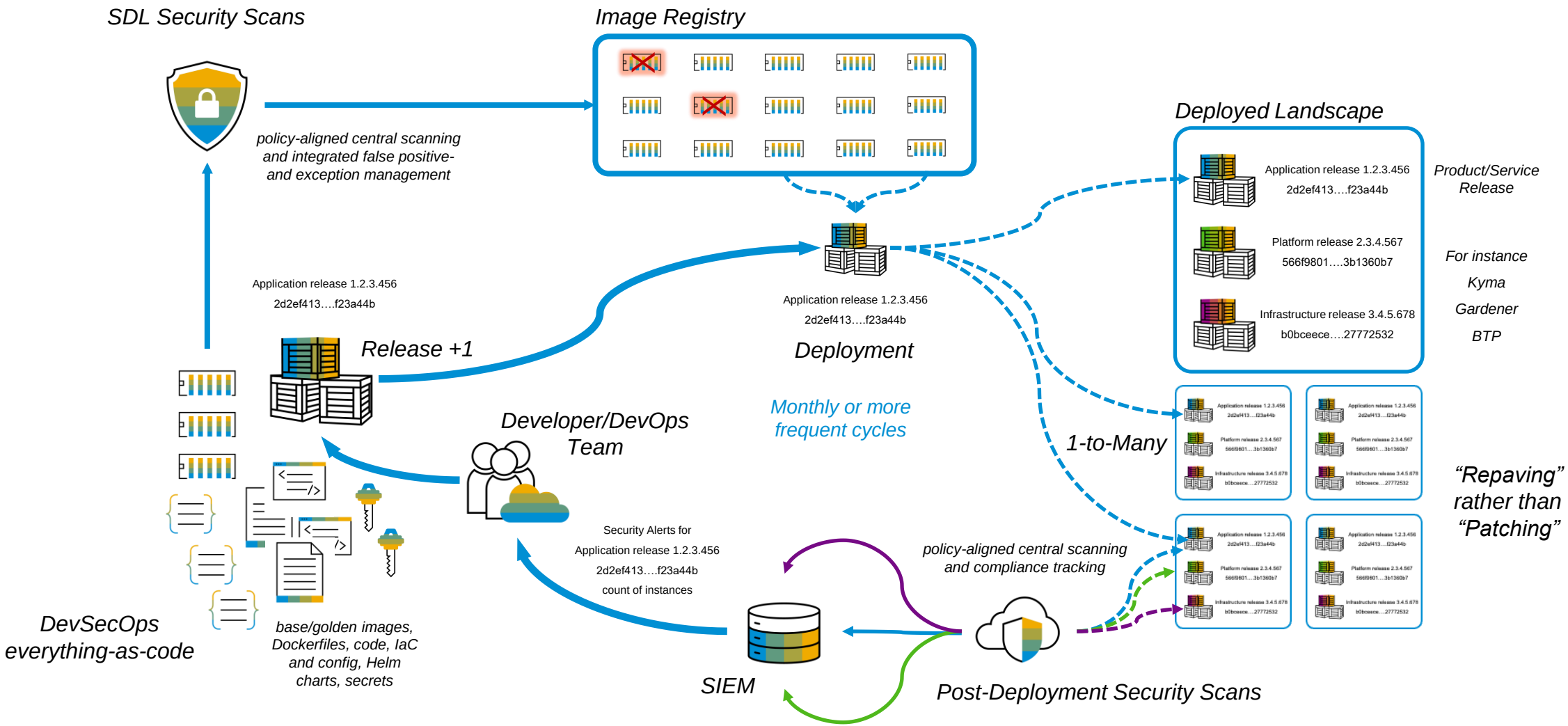
- Oct 1, 2020 announcement SAP accelerates cloud migration for remaining teams by end of 2022
- Continued quadratic growth
- Development and launch of SAP's own CSPM solution

Cloud-native Application Protection Platform

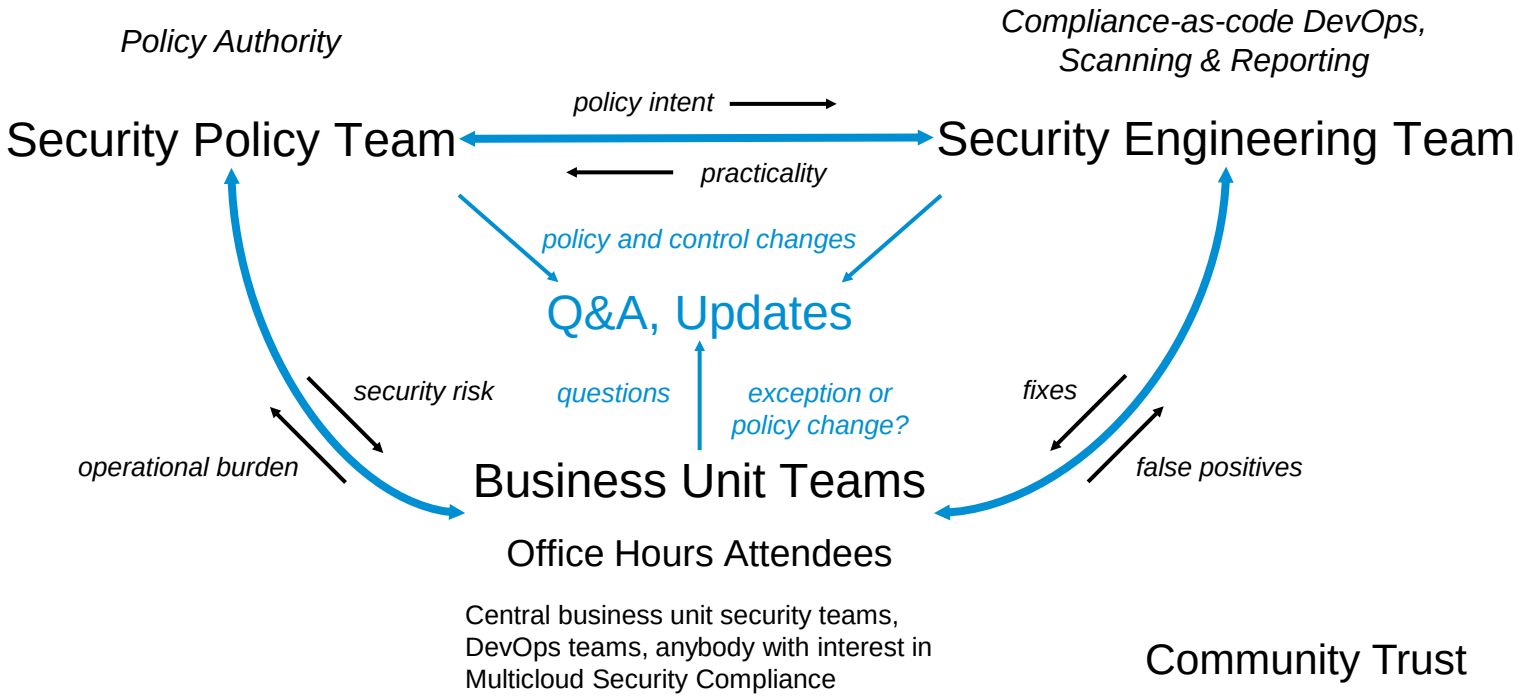
- Selection of CNAPP provider and deployment into landscape
- Operationalization of findings into central services for asset mgt., compliance, vulnerability mgt. and attack surface reduction, threat and malware detection

The Centrality of the Cloud-native Service Lifecycle

DevSecOps – Secure Software Development and Operations Lifecycle



Community Enablement and Engagement Model – Office Hours



Weekly Meeting Open to All Interested

- Voluntary, but drawing regularly 50+ attendees, 100+ on occasion
- Running since August 2019

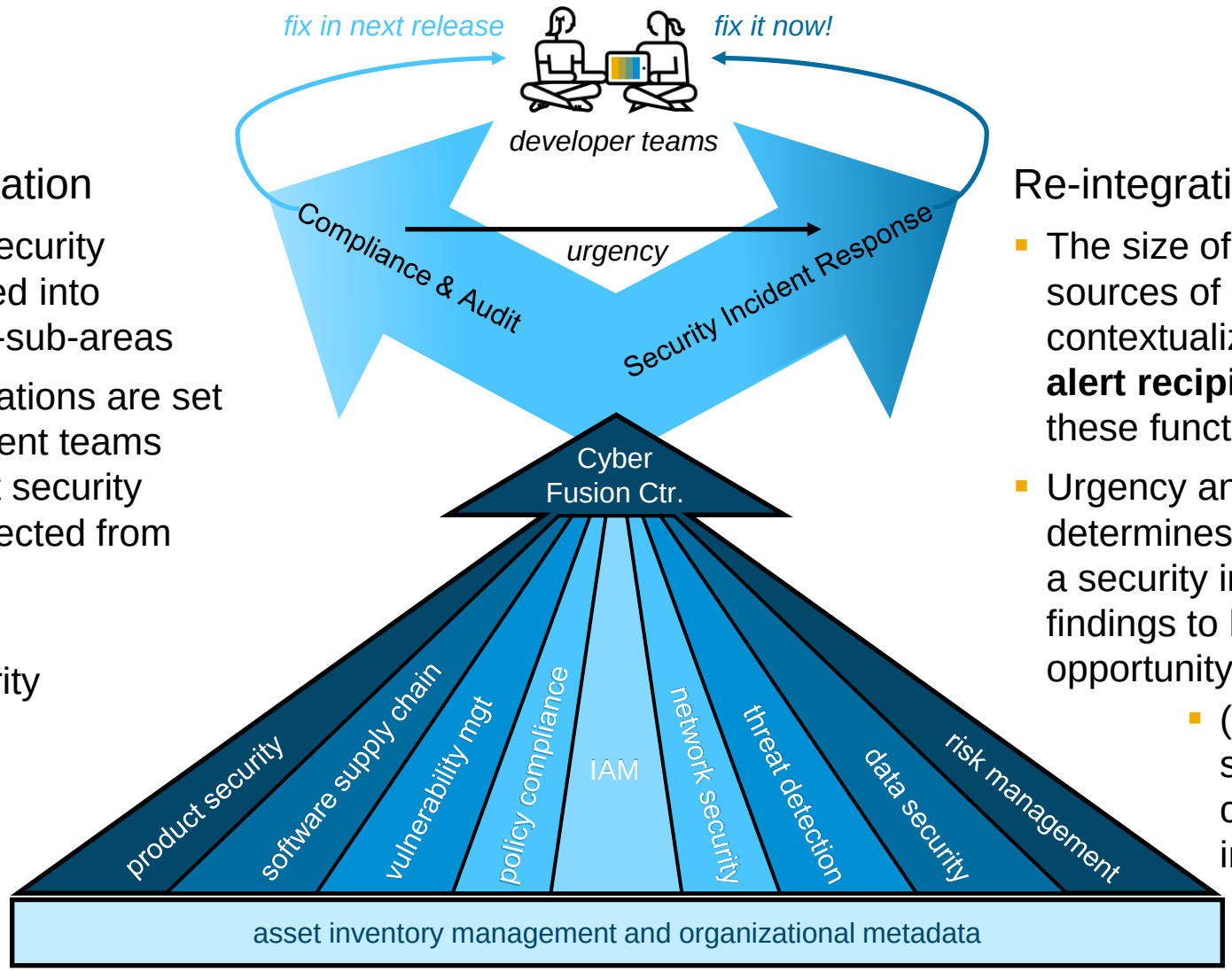
Community Trust

- Fast Response
- Possibly avoiding unnecessary and burdensome exception processes
- Understanding that high rate of change is (largely) community-driven
- Impactful changes debated early and adjusted if needed

Cloud Security is Recentralizing Cybersecurity's Fragmentation

20 Years of Fragmentation

- As Infosec matured, security increasingly fragmented into different sub- and sub-sub-areas
- Many security organizations are set up this way, with different teams taking care of different security topics – often disconnected from each other
- But…, these common sources of cloud security breaches?

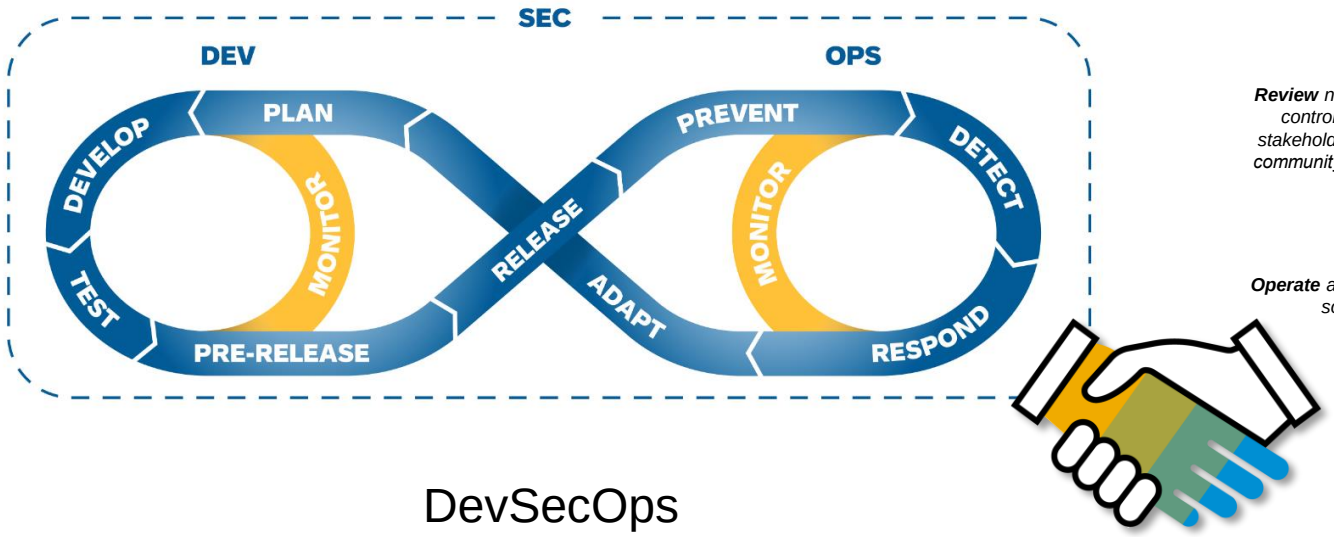


Re-integration for Cloud

- The size of the landscape, the key sources of security breaches, contextualization and, critically, **alert recipients** are re-centralizing these functions
- Urgency and severity of the alert determines whether it is treated as a security incident or a compliance findings to be cycled out at next opportunity
  - (Most) CNAPP solutions specifically useful in this contextualized re-integration

Cloud-native DevSecOps and SecDevOps

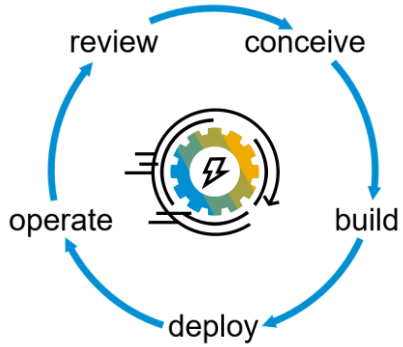
Secure DevOps Practices Paired with DevOps Security Operations for Aligned Agility



DevSecOps

Review *new or updated controls, etc. with stakeholders and wider community, leading to…*

Operate *and monitor the solution*



SecDevOps

Conceive *of new or updates to existing controls, pipelining, etc.*

Develop and ***Build*** *new or update existing controls, pipelining, etc.*

Deploy *the new or updated controls, pipelining, etc. and test across the dev, pre-prod and prod landscapes*

Recommended Reading

Security Chaos Engineering: Sustaining Resilience in Software and Systems,
Kelly Shortridge with Aaron Rinehart, 2023

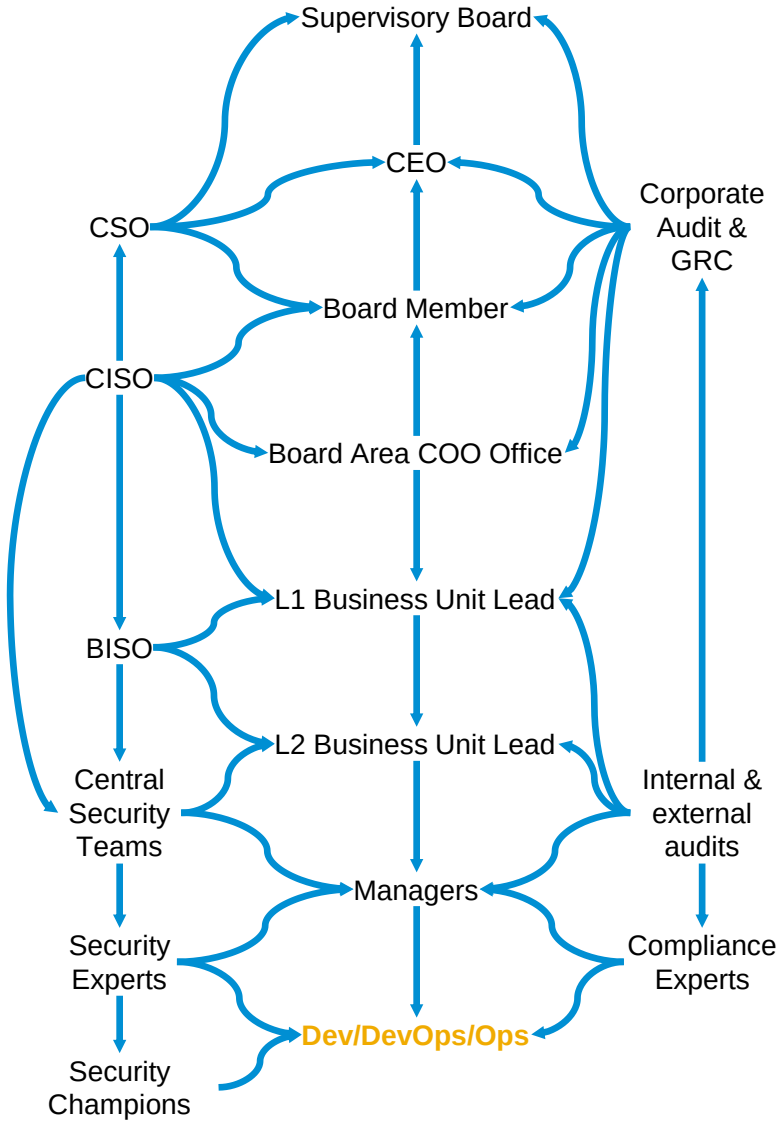
Security Chaos Engineering and Security Engineering Amid Chaos: Cloud-native Cyber Resilience,
SAP Community

Accountability Throughout the Organizational Hierarchy

Making Security Matter

Reporting and SLA Tracking

- Experience shows policies are not followed unless verified
- Central security and compliance scans alone do not make an organization move
- Multi-level reporting and SLA tracking
- Multiple layers of accountability established throughout the organizational hierarchy to ensure alerts are followed up on
- Regular EB/SVB, L1, Board Area Delegate, BISO Council, Office Hours Meetings
- *Quis custodiet ipsos custodes?* Corporate Audit



Cut Through Competing Priorities

- Security competes with many different priorities – both within technical teams as higher up the organizational hierarchy
- Developers and DevOps Engineers don't set priorities – managers do, VPs do
- Security and Audit & Compliance support is needed to ensure priorities are understood

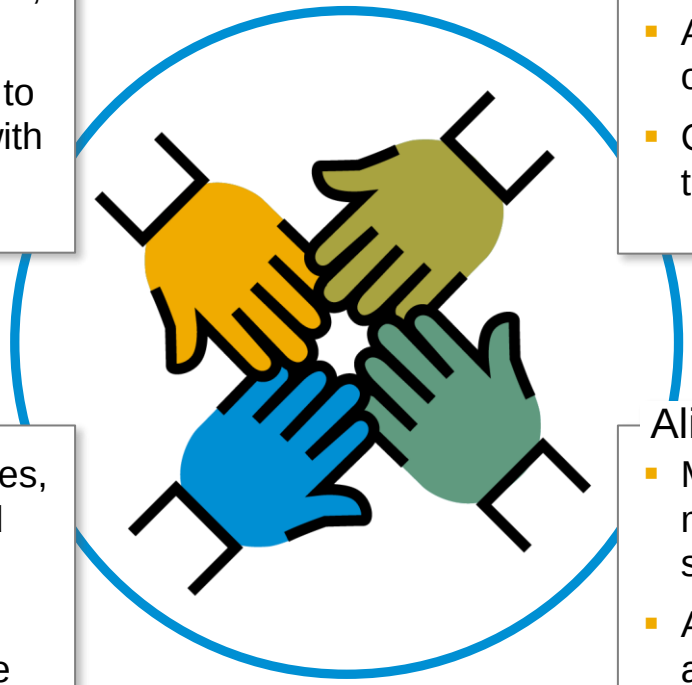
“Shared Fate” – We Are All In This Together

Collaborative

- Operate in a spirit of collaboration across organizational silos and teams
- Keep teams aligned and informed between SGS, LoBs and execution partners
- Leverage engagement and community forums to engage with teams and balance security risk with operational burden and practical constraints

Relieving Operational Burden

- Reduce manual security, compliance and remediation processes that add to operational burden on teams
- Automate processes and central services and optimize for scale, agility and ease of onboarding
- Centralize and automate security scanning, tracking and evidence collection



Enabling

- Support LoB teams with central security services, secure-by-default templates, infrastructure and platforms reducing effort duplication
- Develop and mature partnerships across the organization to align security controls along the Secure Development and Operations Lifecycle
- Nurture an appropriately security-skilled workforce

Aligned Goals and Targets

- Measure on outcome-based metrics and targets of material security improvements – only effective security controls protect us against security risks
- Align SGS success with progress in NIST maturity and security posture encourages collaboration among teams in enablement efforts and relieving operational burden on all parties

SAP NOW

Future Proof Your Business

Save The Date

Date: August 8, 2023

Venue: The Hyatt Regency, Sydney

More details coming soon

Thank you.

Contact information:

Jay Thoden van Velzen

jay.thoden.van.velzen@sap.com
@jaythvv@infosec.exchange
https://www.linkedin.com/in/jay-thoden-van-velzen/

THE BEST RUN SAP