

Security Compliance in Multi Cloud Umgebungen

it-sa 2022 – Patrice Volkmer

NTT DATA und das NTT DATA Partnernetzwerk fokussieren sich auf die Kundenziele – auf lokaler und globaler Ebene.



Top 10

aller weltweit tätigen Business- und IT-Dienstleister.



über 130.000

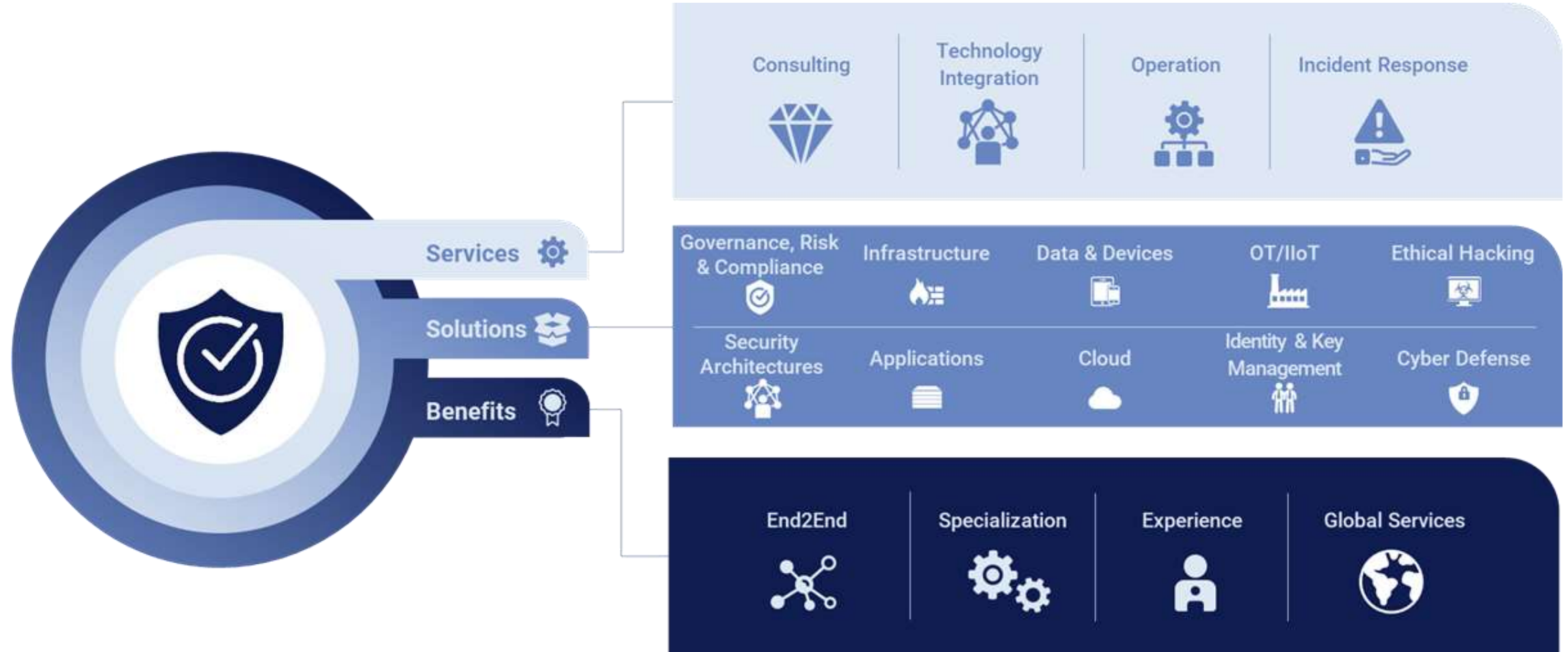
Expert*innen sind in **50** Ländern
auf 6 Kontinenten tätig.



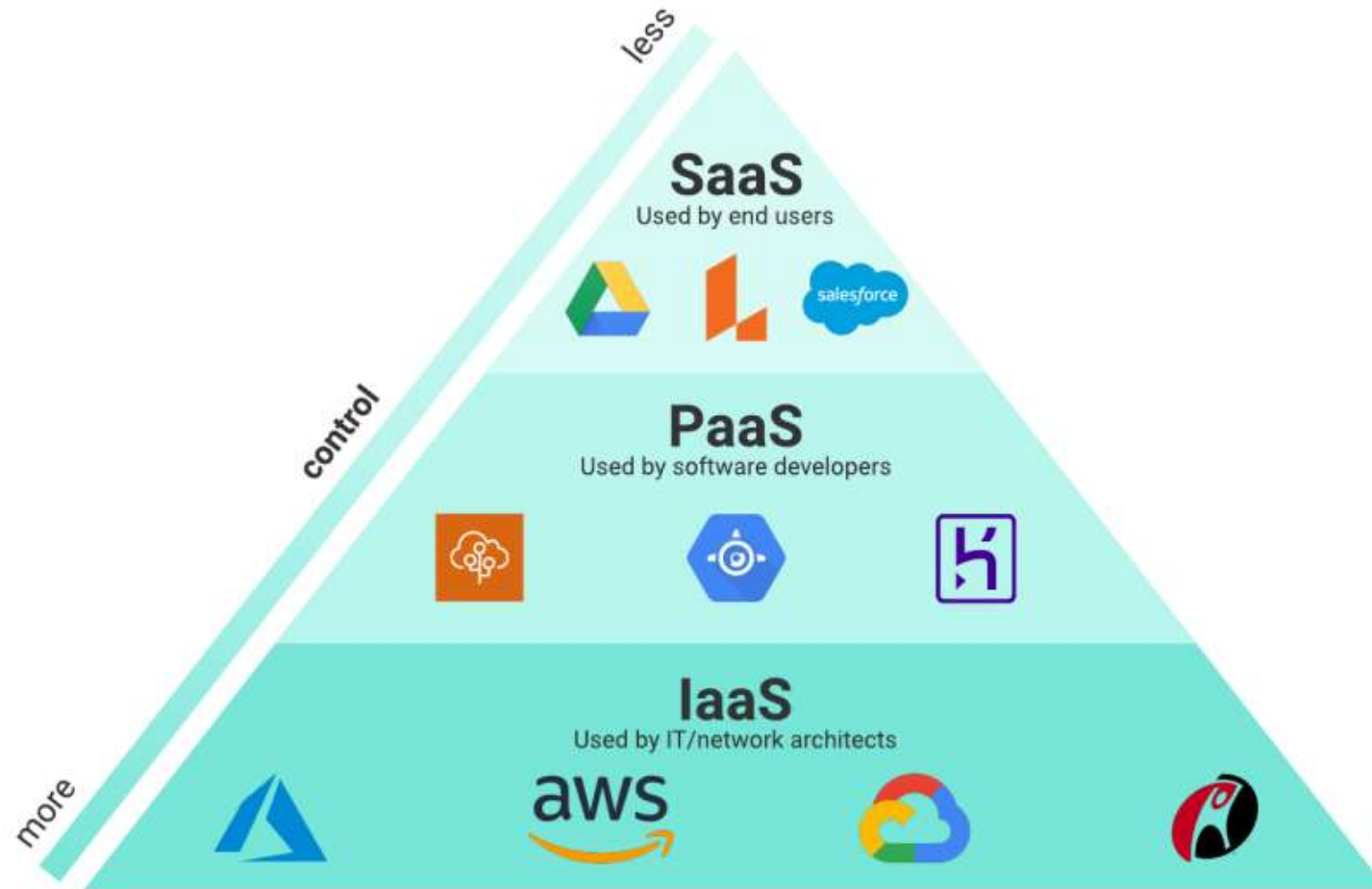
40 %

des globalen Internetverkehrs wird unter hohen
Sicherheitsstandards von NTT gesteuert.

Cybersecurity @ NTT DATA



Cloud – Wolke – Wie genau nun?



Pflicht- themen

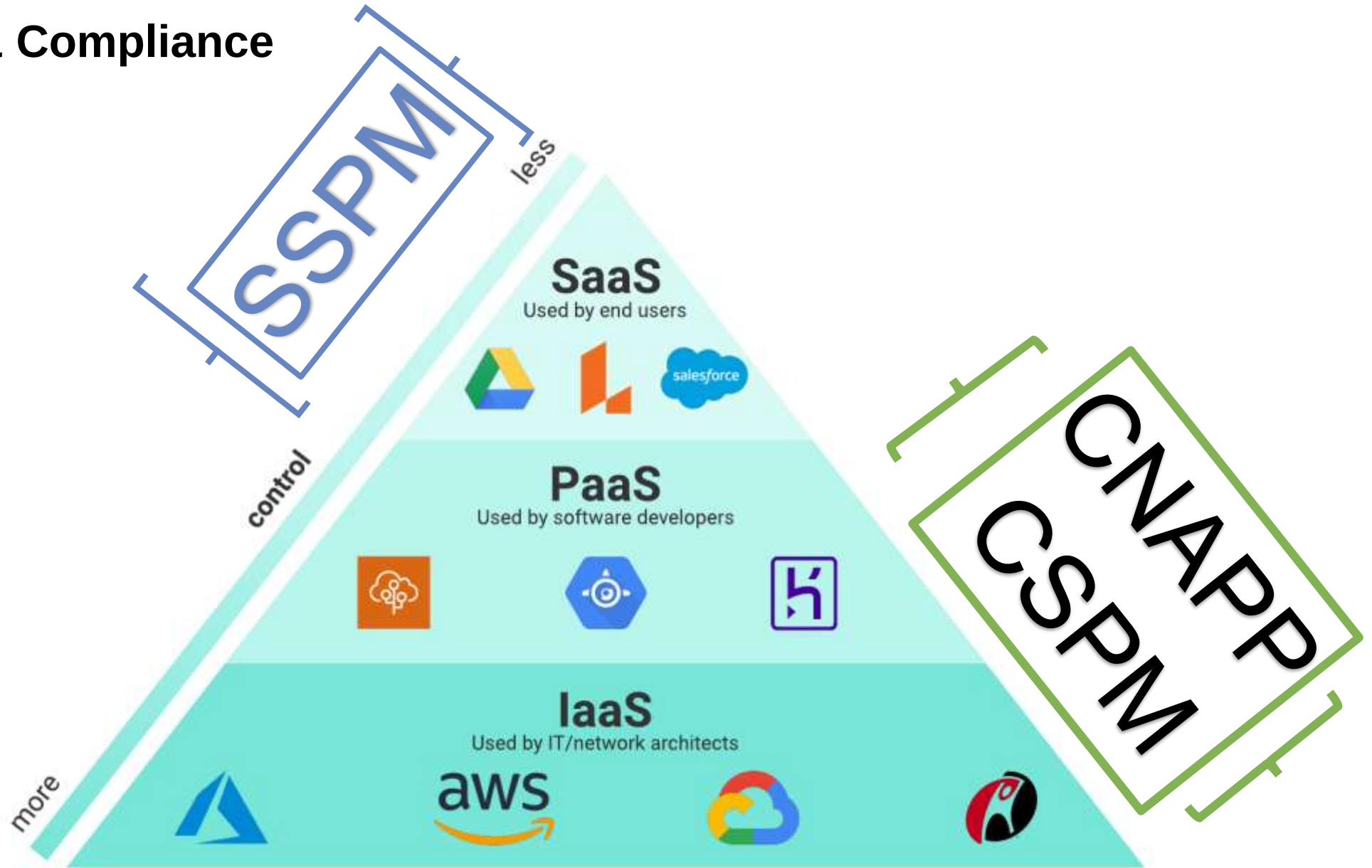
Vorgaben

Standardisierung (Building Blocks)

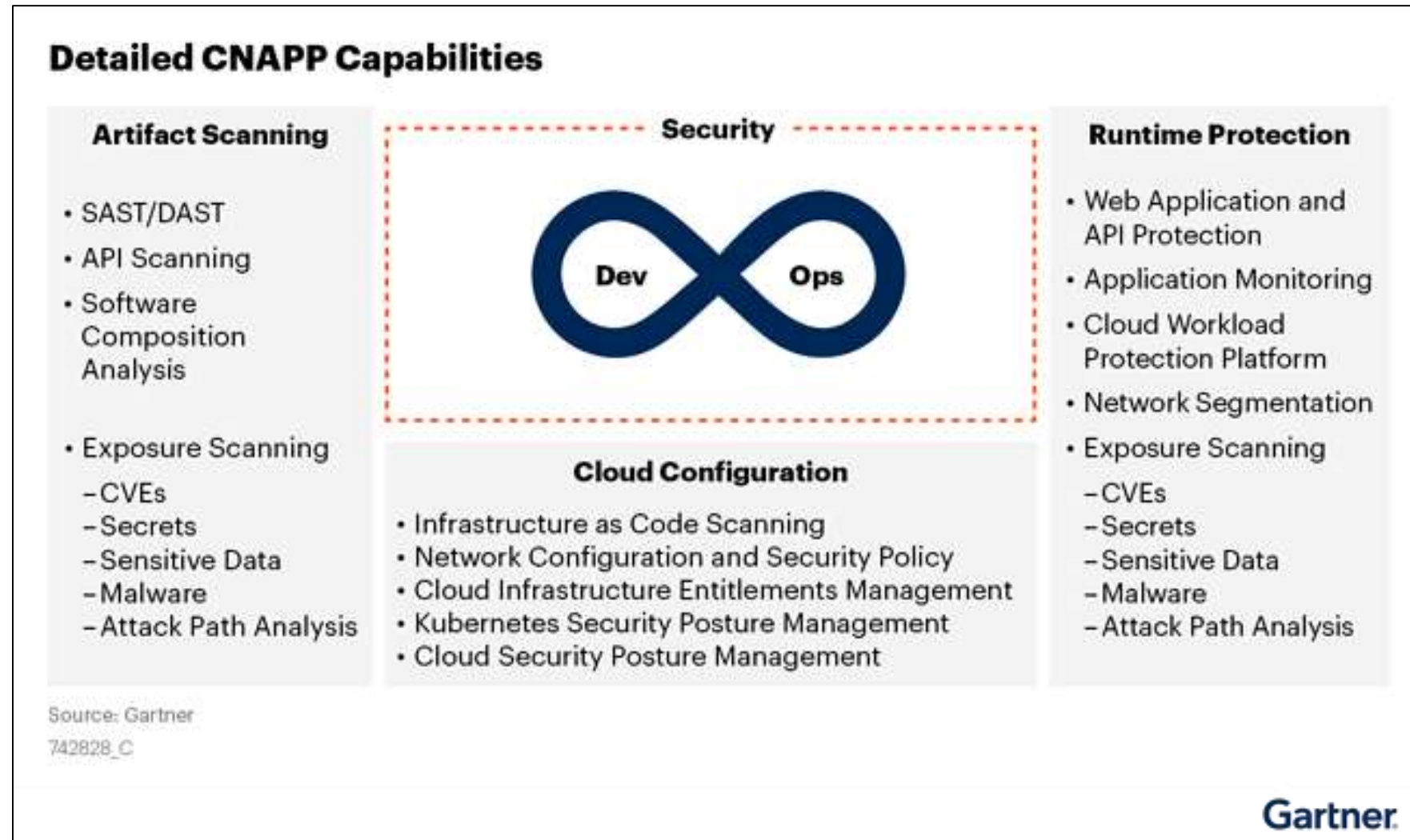
Automatisierung

Evaluierung Security Controls Check bei Building BLocks

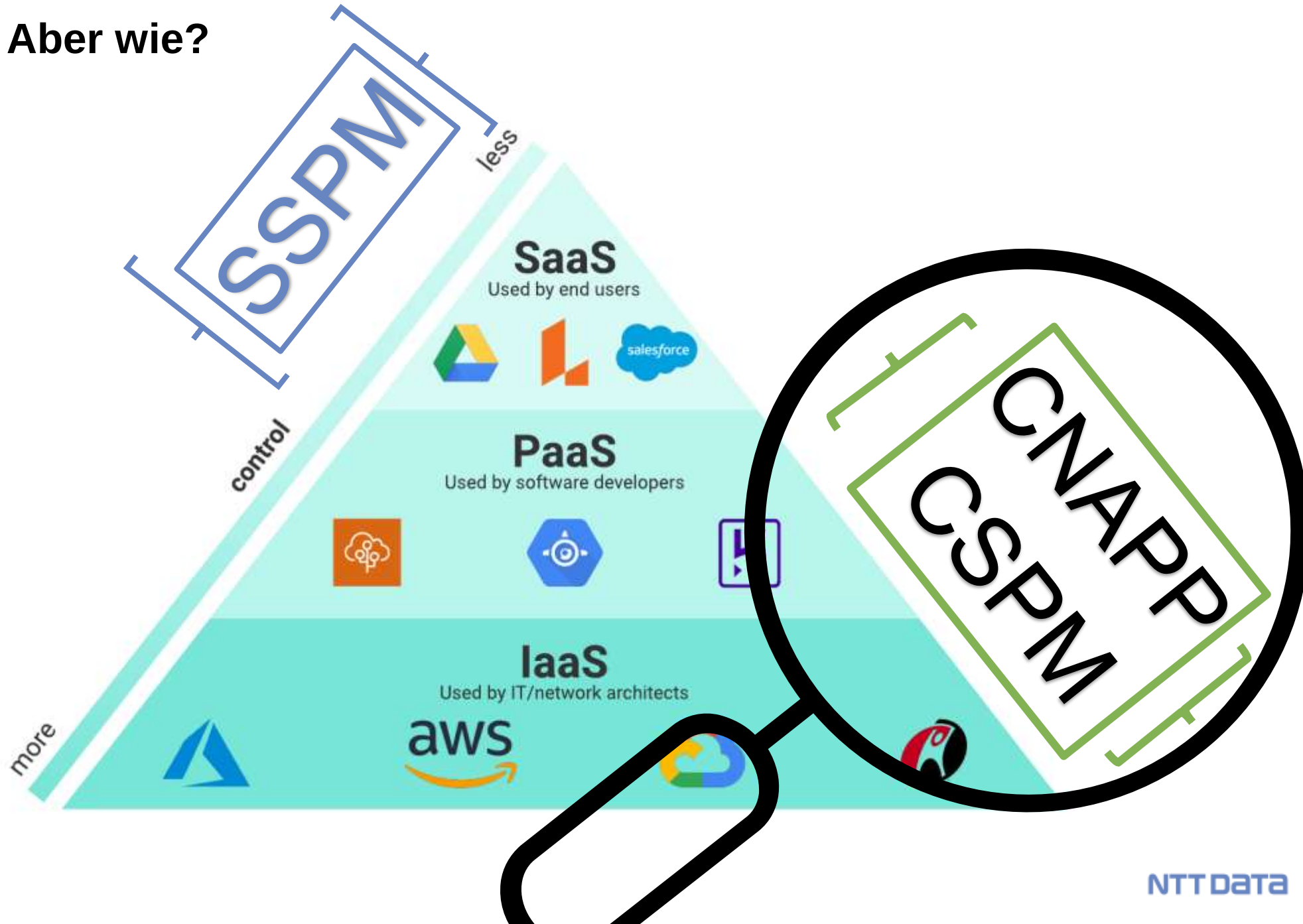
Governance & Compliance Aber wie?



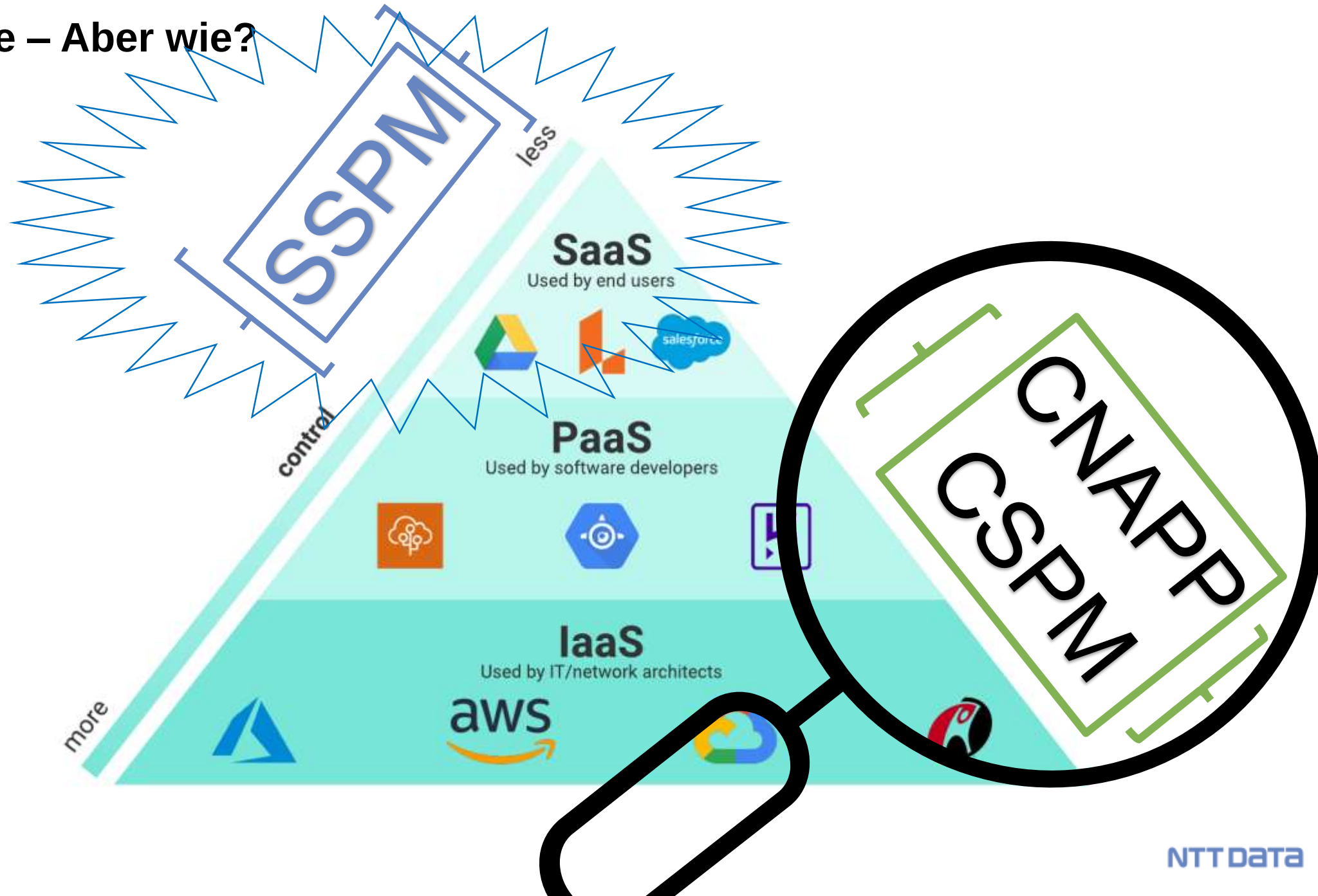
CSPM | CWPP | CSPM



Governance – Aber wie?



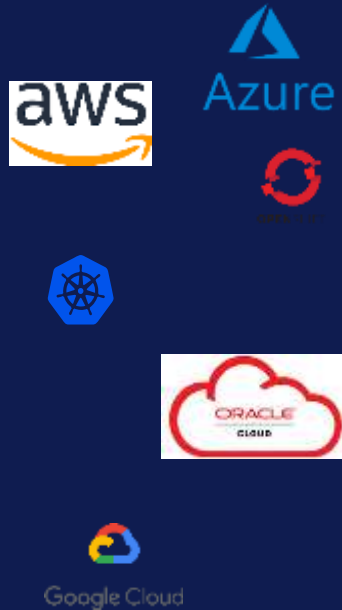
Governance – Aber wie?



Warum ist die Compliance so schwierig zu erreichen

Komplexität

Verschiedene Clouds



Verschiedene Architekturen

Serverless Adoption

39% Of organizations are using **Serverless** technologies.

75% Rely on hosted platforms (e.g. Lambda, Azure Functions) to run **Serverless**.

Kubernetes Adoption

96% Of organizations are either using, or evaluating **Kubernetes**.

90% Of **Kubernetes** users leverage the cloud-managed **Kubernetes** services.

5.6M Developers using **Kubernetes**.

AWS Accounts as Security Boundaries — 97+ Ways Data Can be Shared Across Accounts

© 2021 AWS

© 2021 AWS

Verschiedene Services und Technologien

Cloud Σ Services

aws > 200

Azure > 200

Google Cloud > 170

Verschiedene Risikoursprünge

Vulnerability

CVE-2022-24086: Critical 0-Day Vulnerability Found in Magento 2 and Adobe Commerce

February 9, 2022 10:00 AM

Malicious **Kubernetes** Helm Charts can be used to steal sensitive information from Argo CD deployments

spring

Spring Blog

Spring Framework RCE, Early Announcement

PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034)

Betriebliche Verantwortung



Warum ist es so komplex?

So viele Optionen allein um S3 sicherer zu gestalten

1 Object Ownership [info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

2 Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

3 Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block Public Access settings for this account are currently turned on

Block Public Access settings for this account [info](#) that are enabled apply even if they are disabled for this bucket.

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☒ Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

4 Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) amount of time or indefinitely. [Learn more](#)

☒ Disable

☐ Enable

Permanently allows objects in this bucket to be required in bucket details after bucket creation or overwritten.

Object Lock works only in versioned buckets

5 Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

☐ Disable

☒ Enable

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

☒ Amazon S3-managed keys (SSE-S3)

An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

☐ AWS Key Management Service key (SSE-KMS)

An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

Welche Hyerscaler Lösungen gibt es...

Maecenas porttitor

AWS



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across all of your accounts and regions

Azure

Microsoft Defender for Cloud



Microsoft Defender für Cloud ist eine Lösung für die Verwaltung des Cloudsicherheitsstatus (Cloud Security Posture Management, CSPM) und den Cloud-Workloadschutz (Cloud Workload Protection, CWP); die Schwachstellen in Ihrer Cloudkonfiguration findet, den allgemeinen Sicherheitsstatus Ihrer Umgebung erhöht und Workloads in Multi-Cloud- und Hybridumgebungen vor neuen Bedrohungen schützen kann.

Wie analysieren CNAPP / CSPM Lösungen die Cloud - Umgebungen...



API – basierend

- Einfache Anbindung
- Beschränkung auf die bereitgestellten Informationen
- Ggf. Zeitverzögert



API – basierend + Agent

- Tiefere Analyse der Ressourcen
- Analyse gegenüber Malware etc.
- Limitierung auf unterstützte Agenten
- Ggf. Beeinflussung der Umgebungen



API – basierend + Agentenlose Tiefenanalyse

- Tiefe Analyse
- Nicht inversiv
- Für Überwachung von Auslagerungen geeignet

Fokussierung auf Risikohafte Fehlkonfigurationen durch Cross Asset und Cross Hyperscaler Korrelation

Wie analysieren CNAPP / CSPM Lösungen die Cloud - Umgebungen...



API – basierend

- Einfache Anbindung
- Beschränkung auf die bereitgestellten Informationen
- Ggf. Zeitverzögert



API – basierend + Agent

- Tiefere Analyse der Ressourcen
- Analyse gegenüber Malware etc.
- Limitierung auf unterstützte Agenten
- Ggf. Beeinflussung der Umgebungen



API – basierend + Agentenlose Tiefenanalyse

- Tiefe Analyse
- Nicht inversiv
- Für Überwachung von Auslagerungen geeignet

Fokussierung auf Risikohafte Fehlkonfigurationen durch Cross Asset und Cross Hyperscaler Korrelation

Kontakt – Uns finden Sie in der Halle 7 - Standnummer {7-126} & {7-128}



Halle 7 - Standnummer {7-126} & {7-128}
Head of Application Security | Cybersecurity DACH

Zettachring 2
70567 Stuttgart

Patrice.Volkmer@nttdata.com

M: +49 172 1032 920



