



Zero Trust
Data Security™

You are under Attack!!!

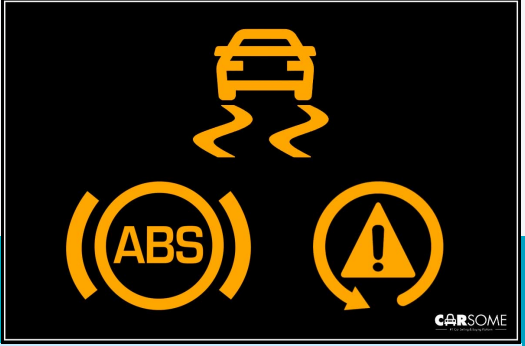
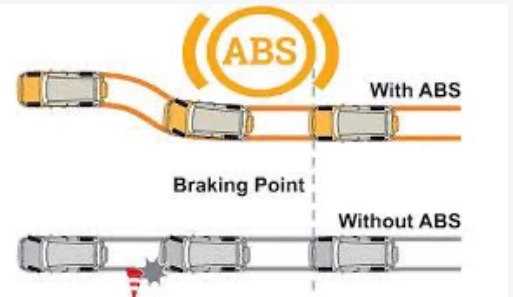
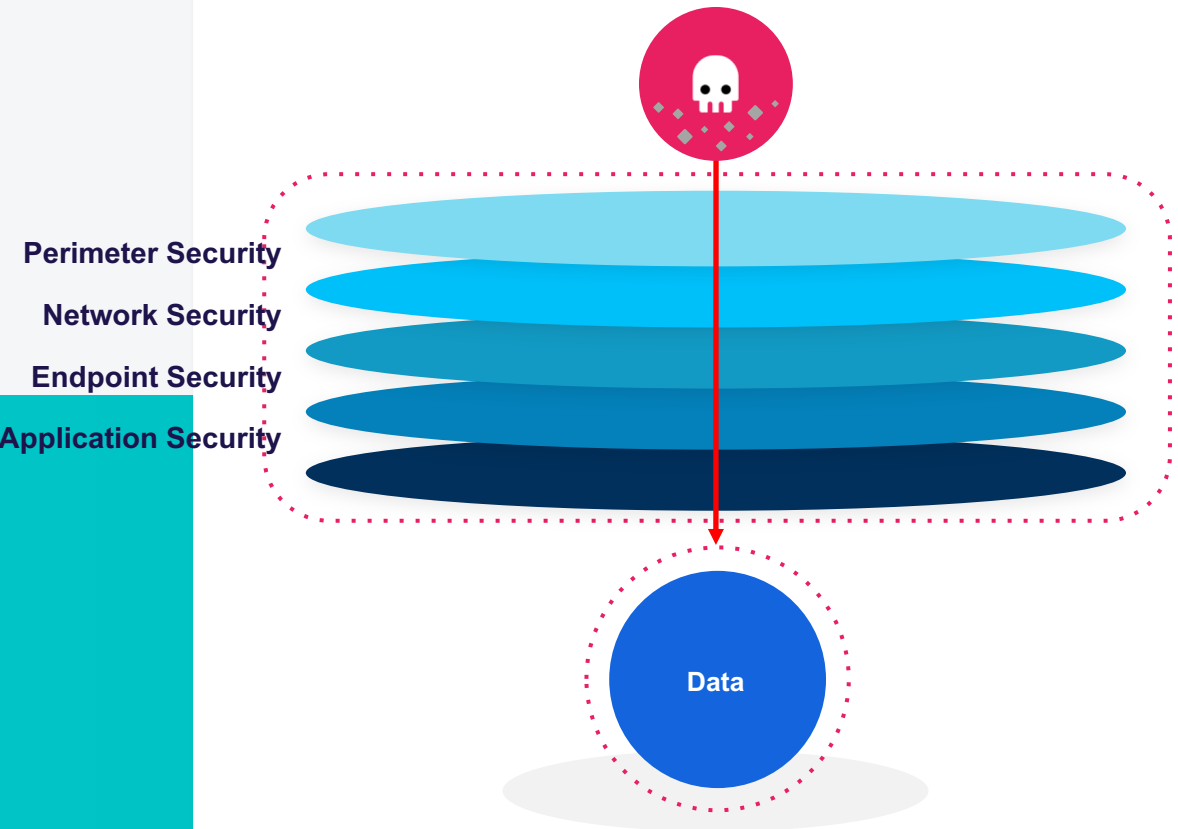
Backup ≠ Cyber Recovery for DC, Cloud, SaaS & K8

Peter Eriksson
Rubrik Architect Nordics

**DON'T
PAY THE
RANSOM**

Businesses are under attack & they all have Security

“Assume Breach”



What's your last defence?



PWC CEO Survey

CEO Survey 2022: Positiv syn på tillväxt skuggas av lågt engagemang för klimatet

PwC:s tjugofemte årliga vd-undersökning

Årets rapport bygger på insikter från 4 446 företagsledare från 89 länder.



77%

av företagsledarna tror på ökad global tillväxt det kommande året

49%

av respondenterna i undersökningen oroar sig **mest** för cyberhot

26%

av de g
åttagan
plats



Anna Renneus Guthrie
anna.reneusguthrie@tn.se

Publicerad: 3 feb 2023, 07:02
Uppdaterad: 3 feb 2023, 09:42

CYBERATTACKERNA

Experter: Cyberkriget mot Sverige trappas upp – så skyddar du dig



Natoprocessen och kraftiga reaktioner från omvärlden har ökat säkerhetsriskerna. Sverige och Europa är inte "tillräckligt förberedda" på nästa fas i hybridkriget, menar experter. Genrebild/Montage. Bild: Mostphotos

Enligt ["Cyberbrott mot svenska företag" \(2022\)](#) av Sevenska handelskammaren så halkar Sverige efter i flera säkerhets-index och hamnar på plats 15 i Europa och 26 Globalt Källa: [Global Cyber Security Index](#) .

Recent attacks in the Nordics

EASYPARK

News Our offer About us Career

- **2022 Ransomware Report** – Global ransomware damage costs are predicted to reach \$265 billion by 2031, up from \$20 billion in 2021. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years. A ransomware attack is expected to strike a business or consumer every 2 seconds by 2031, up from every 11 seconds in 2021.

The State of K8s Software Supply Chain Attacks

June 7, 2022 cloud-native architecture, container security, kubernetes, microservices, supply chain security



by Bill Doerrfeld

Securing the software supply chain is in the zeitgeist, and for a good reason. Software supply chain attacks grew by more than 300% from 2020 to 2021. Supply chain attacks continue to surge in recent months, targeting open source software, container images and packages within the CI/CD pipeline. As a result, malicious container images continue to rise and

Statistik Naturvårdsverket – system nere

6 OKTOBER 2022 PUBLICERAD 6 OKTOBER 2022

Naturvårdsverket har utsatts för ett dataintrång och information har läckt från myndigheten som nu inte går att nå digitalt. Det är inte att nå Naturvårdsverket utifrån nu, för att begränsa skadorna från pågående attacker, säger förvaltningschef Håkan Svaleryd.

Naturvårdsverket upptäckte på onsdagseftermiddagen att man hade ett dataintrång.

Det är kod som inte skulle vara i våra system, säger Håkan Svaleryd, som är förvaltningsavdelningen på Naturvårdsverket.

En del av attacken som inleddes upptäcktes också att information från databaserna hade läckt.

Det är information förts över till en server utanför Naturvårdsverket. I nuläget vet vi inte vilken typ av information det rör sig om, säger Svaleryd.



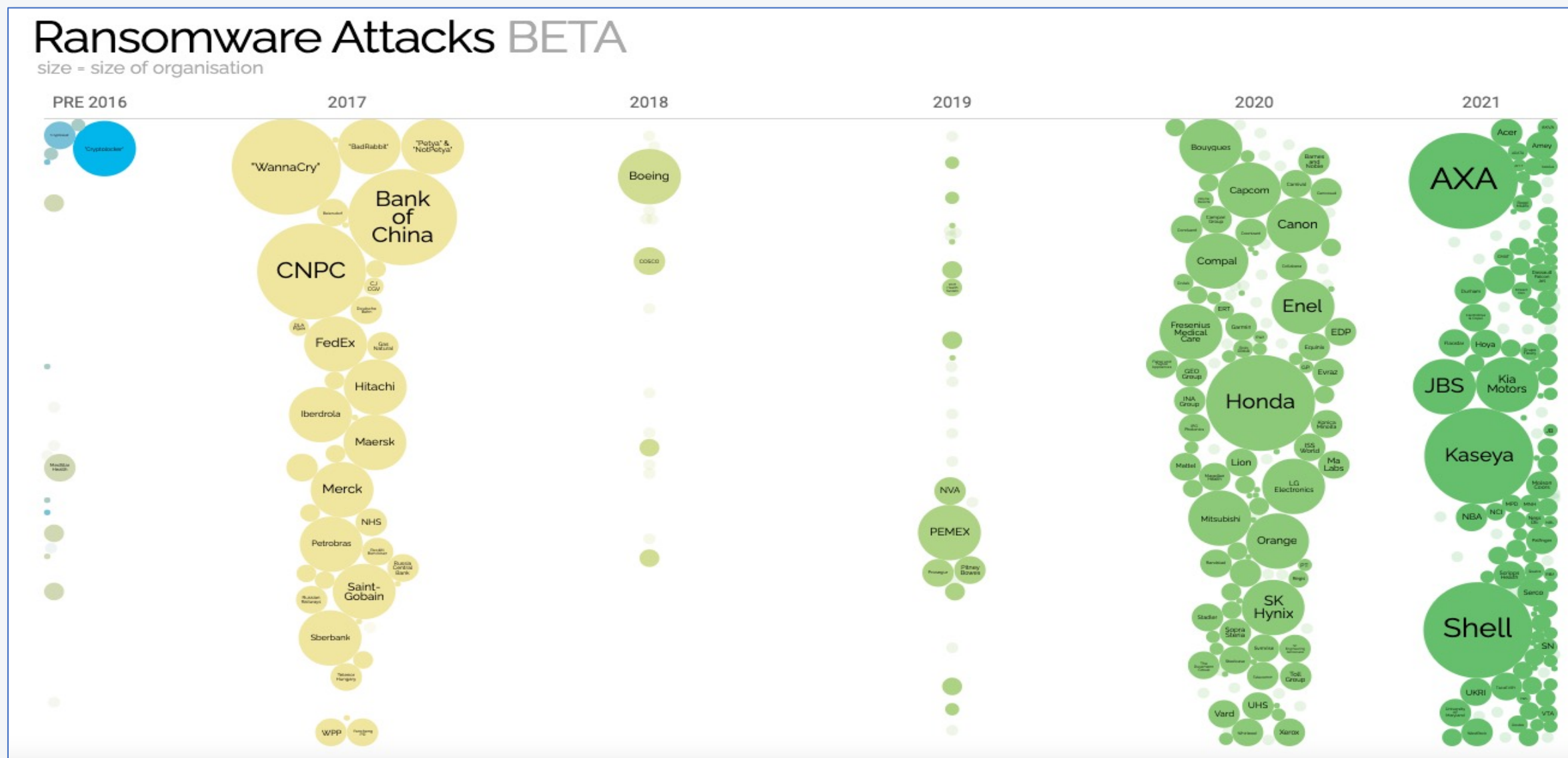
ck

n the

ctors



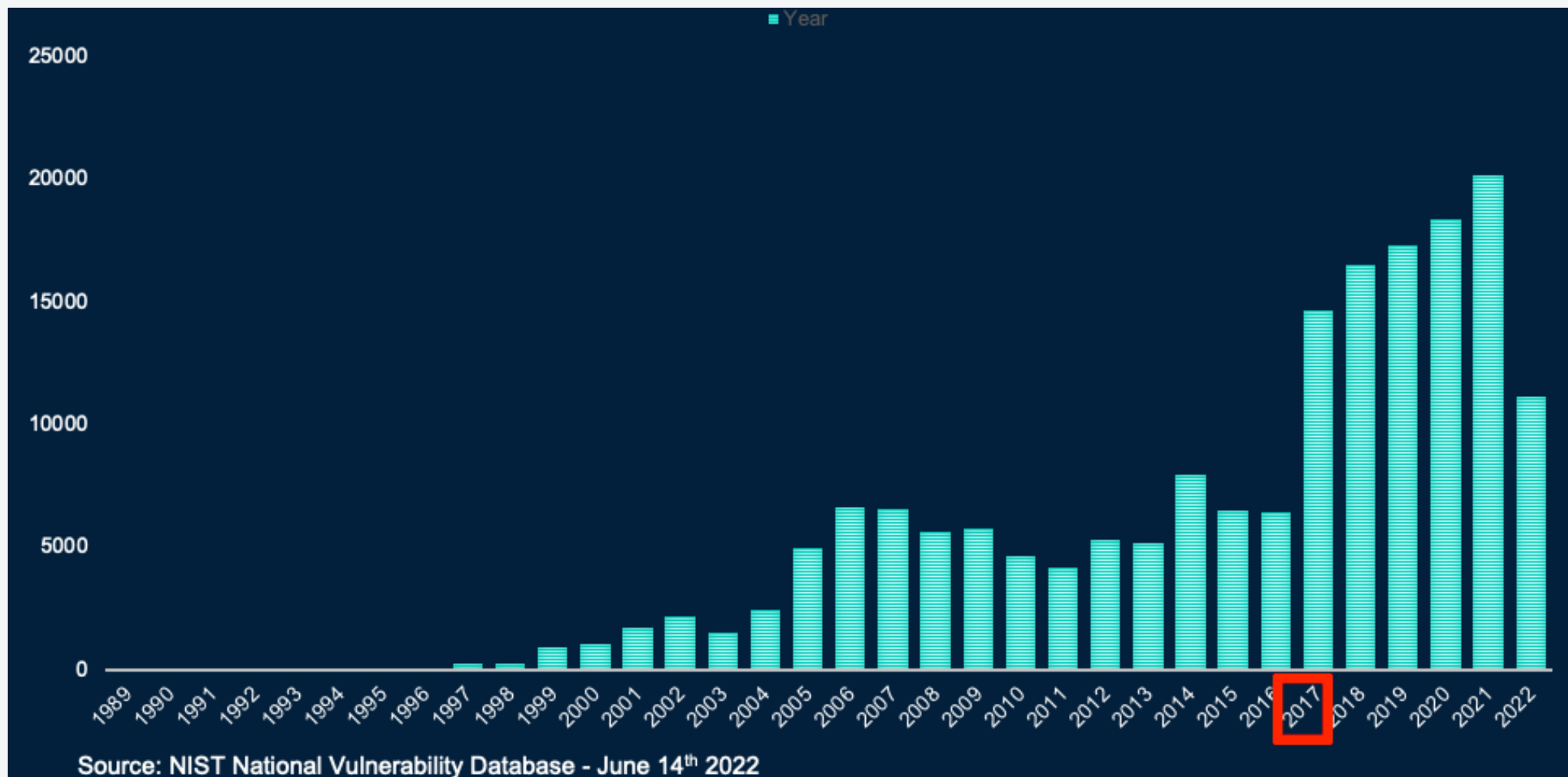
Challenge to keep environment secure- Lots of Patching





Challenge to keep environment secure

Lots of Patching



Not eaiser in a Cloud Native landscape

The image displays a vast collection of cloud native technologies, organized into several functional categories:

- App Definition and Development:** Includes Database (e.g., KV, Viteess, Cockroach Labs, Couchbase), Streaming & Messaging (e.g., cloudevents, NATS, nifi), Application Definition & Image Build (e.g., HELM, Buildpacks.io, OPERATOR FRAMEWORK), and Continuous Integration & Delivery (e.g., argo, flux, agola).
- Orchestration & Management:** Includes Scheduling & Orchestration (e.g., kubernetes, Crossplane), Coordination & Service Discovery (e.g., CoreDNS, etcd), Remote Procedure Call (e.g., gRPC), Service Proxy (e.g., envoy, CONTOUR), API Gateway (e.g., EMISSARY INGRESS, AKANA), and Service Mesh (e.g., LINKERD, Istio).
- Runtime:** Includes Cloud Native Storage (e.g., ROOK, LONGHORN), Container Runtime (e.g., cri-o, Firecracker), and Cloud Native Network (e.g., cilium, CNI).

Each technology is represented by its logo and often includes its CNCF status (e.g., CNCF Graduated, CNCF Incubating).



Zero Trust
Data Security™

You are under Attack!!!

Backup ≠ Cyber Recovery

Peter Eriksson
Rubrik Architect Nordics

**DON'T
PAY THE
RANSOM**



Why security teams are losing trust in the term ‘zero trust’

A key framework for how to secure against modern cyberattacks, zero trust has seen surging interest from business leaders — and been prone to misuse by many vendors.

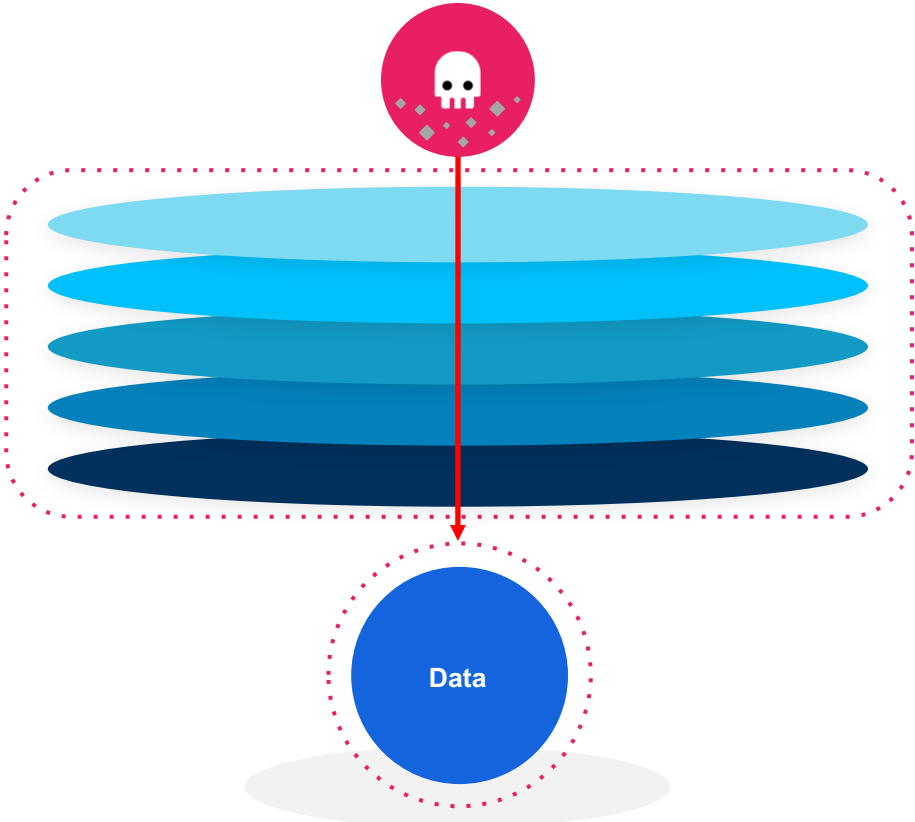
That’s because zero trust is not something you can buy in one package. There are plenty of tools that can help an organization start to embrace the concept — including across identity security, access management, and network segmentation — but no single product that can deliver the whole thing.

Alex Weinert, vice president and director of identity security at Microsoft, has a favorite quote on zero trust, he said during a recent online panel hosted by Protocol. Weinert once asked a chief information security officer to define zero trust, and the answer he received was, “It means whatever the person on the other side of the table is trying to sell.”

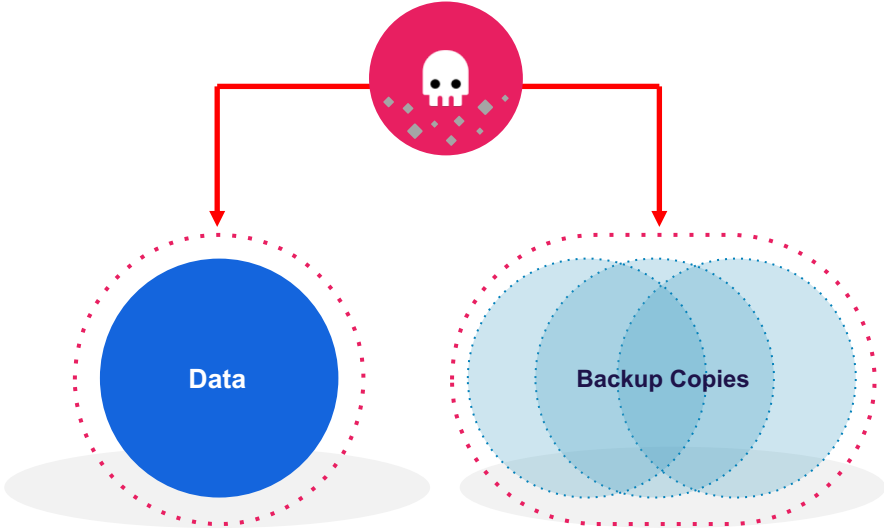
Less flippantly, zero trust can be seen as an organizing principle for how to stop modern cyberattacks. Today attackers tend to follow a certain trajectory: After gaining initial access to an environment, they move around on the network, take over additional accounts, and elevate their account privileges to let them take additional, more damaging actions.

Businesses are Under Attack

“Assume Breach”



Data and Backup are the targets



Why security teams are losing trust in the term ‘zero trust’

A key framework for how to secure against modern cyberattacks, zero trust has seen surging interest from business leaders — and been prone to misuse by many vendors.

That’s because zero trust is not something you can buy in one package. There are plenty of tools that can help an organization start to embrace the concept — including across identity security, access management, and network segmentation — but no single product that can deliver the whole thing.

Alex Weinert, vice president and director of identity security at Microsoft, has a favorite quote on zero trust, he said during a recent online panel hosted by Protocol. Weinert once asked a chief information security officer to define zero trust, and the answer he received was, “It means whatever the person on the other side of the table is trying to sell.”

Less flippantly, zero trust can be seen as an organizing principle for how to stop modern cyberattacks. Today attackers tend to follow a certain trajectory: After gaining initial access to an environment, they move around on the network, take over additional accounts, and elevate their account privileges to let them take additional, more damaging actions.

Who can you trust?

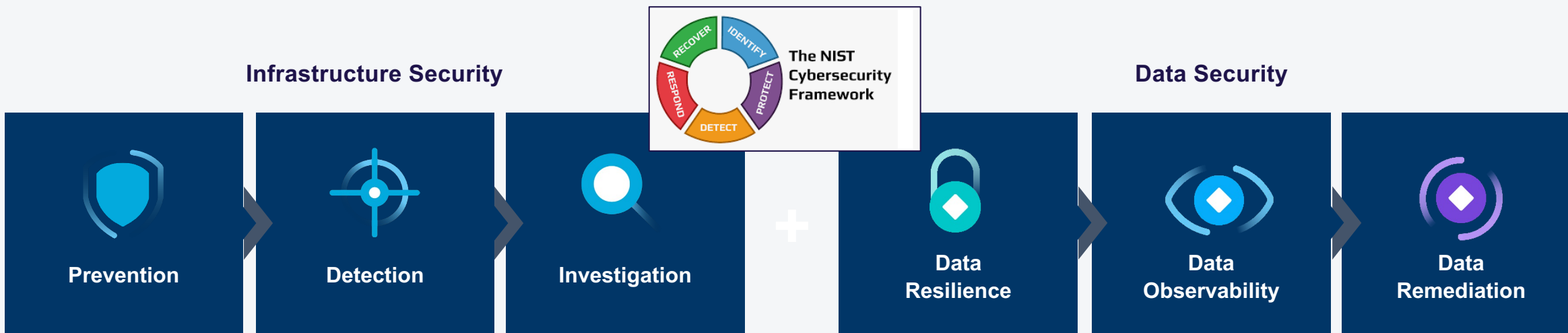
Kapil Raina, vice president of zero trust marketing at CrowdStrike, has a rule of thumb for determining if a product has anything to do with zero trust or not: Check it against the National Institute of Standards and Technology.

<https://www.protocol.com/enterprise/security-zero-trust-cloudflare-zscaler>



The Next Frontier in Cybersecurity

Infrastructure Security And Data Security Together Provide Zero Trust Security



Rubrik



That's because zero trust is not something you can buy in one package. There are plenty of tools that can help an organization start to embrace the concept – including across identity security, access management, and network segmentation – but no single product that can deliver the whole thing.

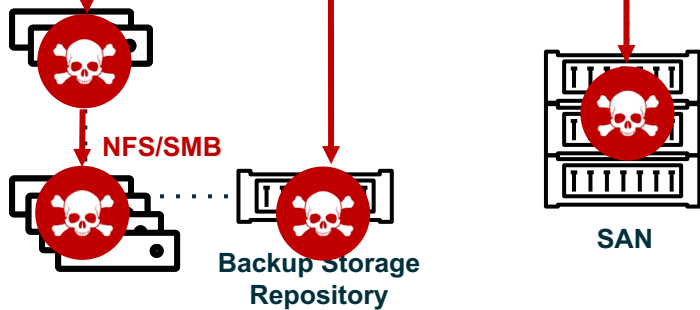
Is Your DC Data an Easy Target?



Legacy Backup Server
(Master, Catalog)

Backup Proxy
(Ingest, Mover)

- 2 cores min
- 1 core per job
- 2 GB RAM
- 12 GB for 50 jobs



Search / Index

- Separate Windows Server
- MS SQL License
- Potential SPOF



Monitoring/Reporting

- Req'd for Monitoring
- Req'd for Reporting



Enterprise Server

- Global View/Mgmt
- API integration point



Gateway Server (Replication)

- Data mover
- Move replicated data or archived data
- WAN Optimization



O365 Backup Proxy

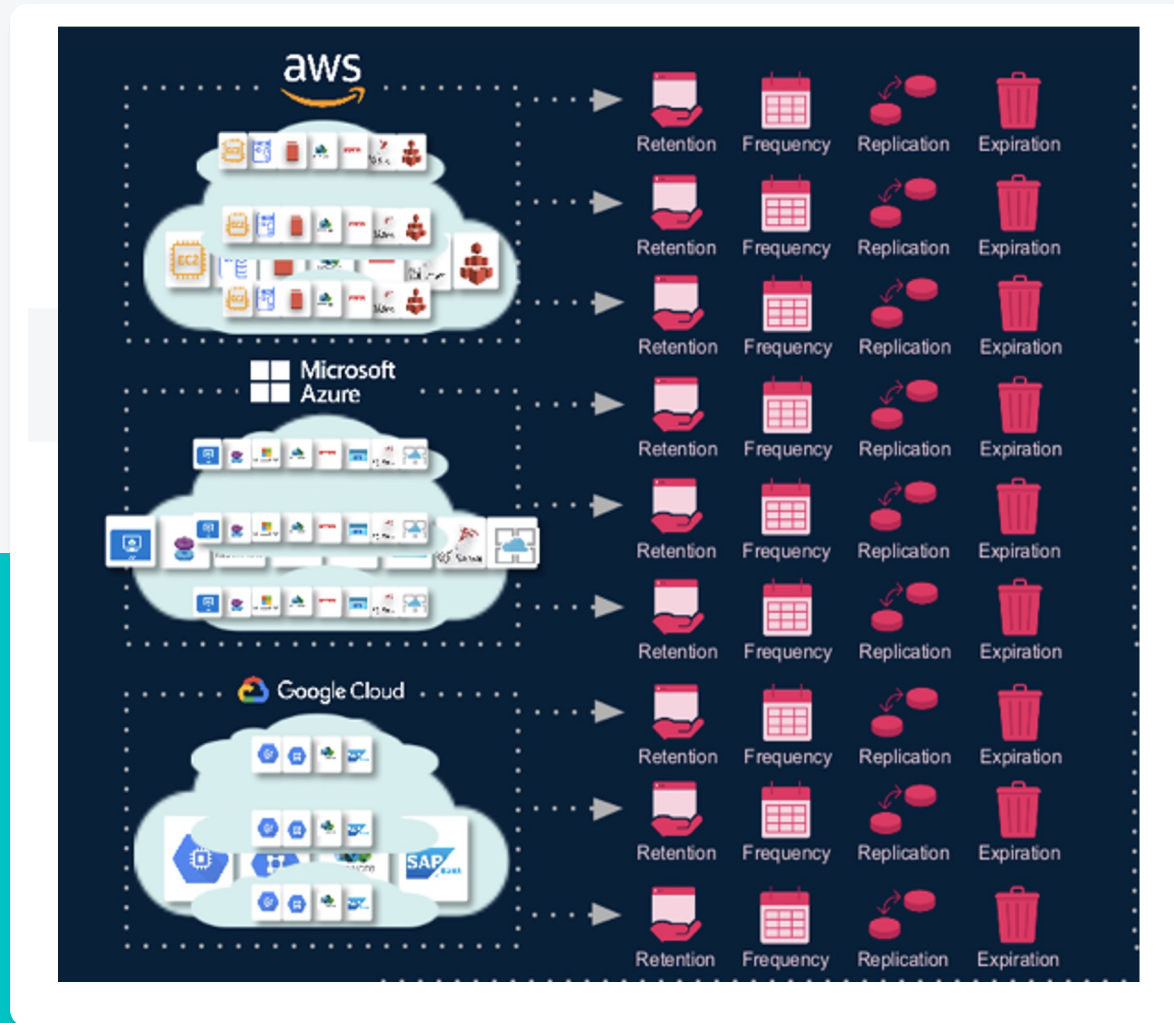
- Pull Data back over WAN
- Store all backups on-prem

Might not be designed for threats inside your network

- Are the network protocols open?
- What is running windows or on insecure components?
- Is MFA and TOTP deployed and enforced?
- Is NTP secured?

**Assume
Breach**

But we have cloud & K8?



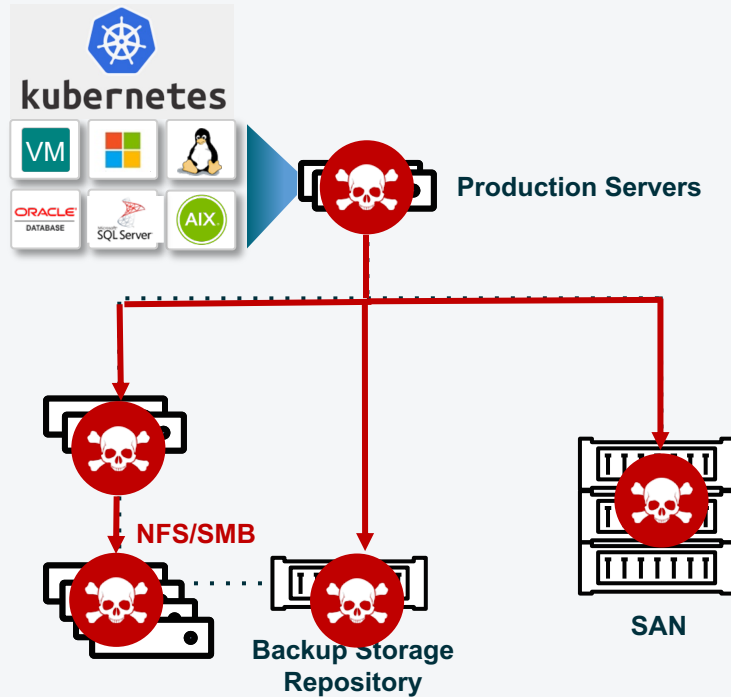
Cloud: New Questions

- What exactly do I recover?
- Was sensitive data in scope?
- How do I ensure I don't restore the malware?

**Assume
Breach**

Legacy vs Rubrik Are your data a easy target?

Legacy – Insecure



Legacy Backup Server
(Master, Catalog)

Backup Proxy
(Ingest, Mover)

- 2 cores min
- 1 core per job
- 2 GB RAM
- 12 GB for 50 jobs



- Search / Index**
- Separate Windows Server
 - MS SQL License
 - Potential SPOF

- Monitoring/Reporting**
- Req'd for Monitoring
 - Req'd for Reporting

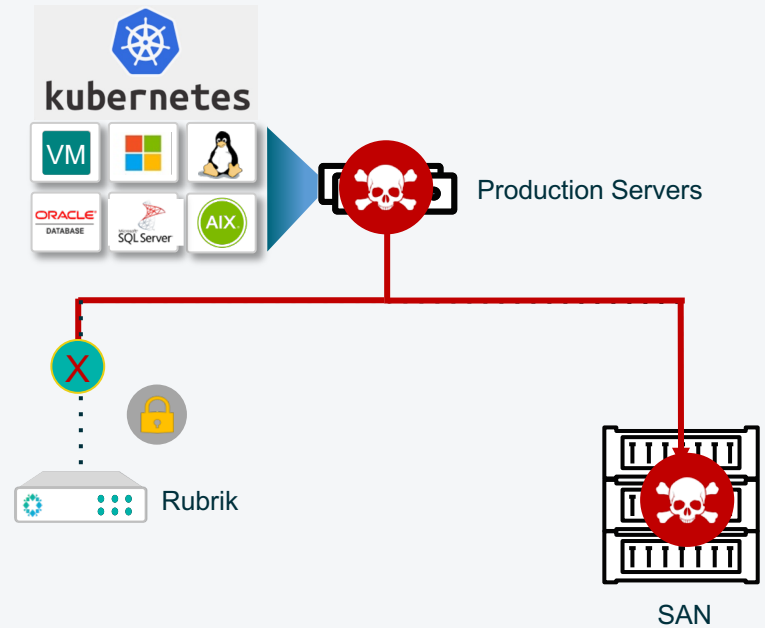
- Enterprise Server**
- Global View/Mgmt
 - API integration point

- Gateway Server (Replication)**
- Data mover
 - Move replicated data or archived data
 - WAN Optimization

- O365 Backup Proxy**
- Pull Data back over WAN
 - Store all backups on-prem



Rubrik Arhchitectoral Security - Air Gap



Secure communication and an immutable file system ensures data in Rubrik can never be tampered with directly over the network

Distributed, Masterless, Scale-Out Architecture

Master-less cluster

2U/4Node

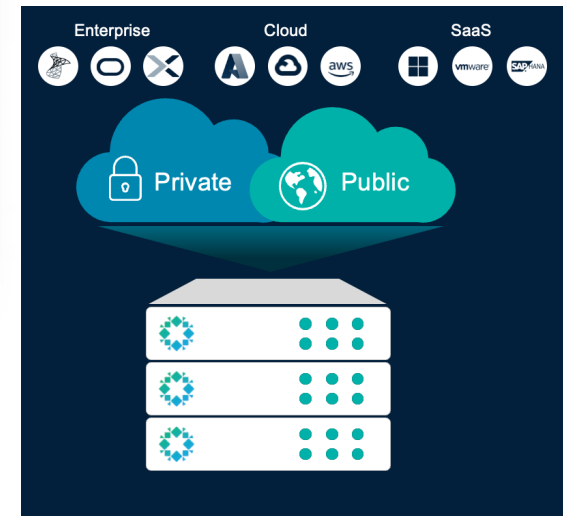
Self-healing architecture



Cloud-scale

API-first architecture

Distributed filesystem



Rubrik Data Resilience (Bunker-in-box)

Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups



Intelligent Data Lock – so they can't destroy it

Intelligent recycle-bin holds all data for 7+ days beyond last admin action

Retention Lock – so they can't disrupt backups

Two-person approval needed to change retention policies

Access Control at Every Level – so they can't access it

Granular RBAC and mandatory, natively enforced MFA and TOTP

Logical Air Gap - so they can't find it

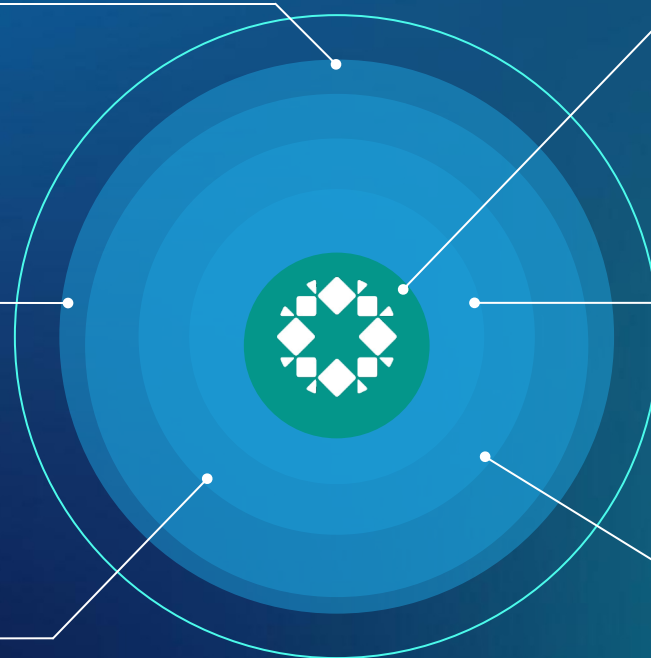
Undiscoverable with NFS/SMB Network Protocols

Encryption Everywhere – so they can't see it

Strong encryption of data at-rest and data in-flight

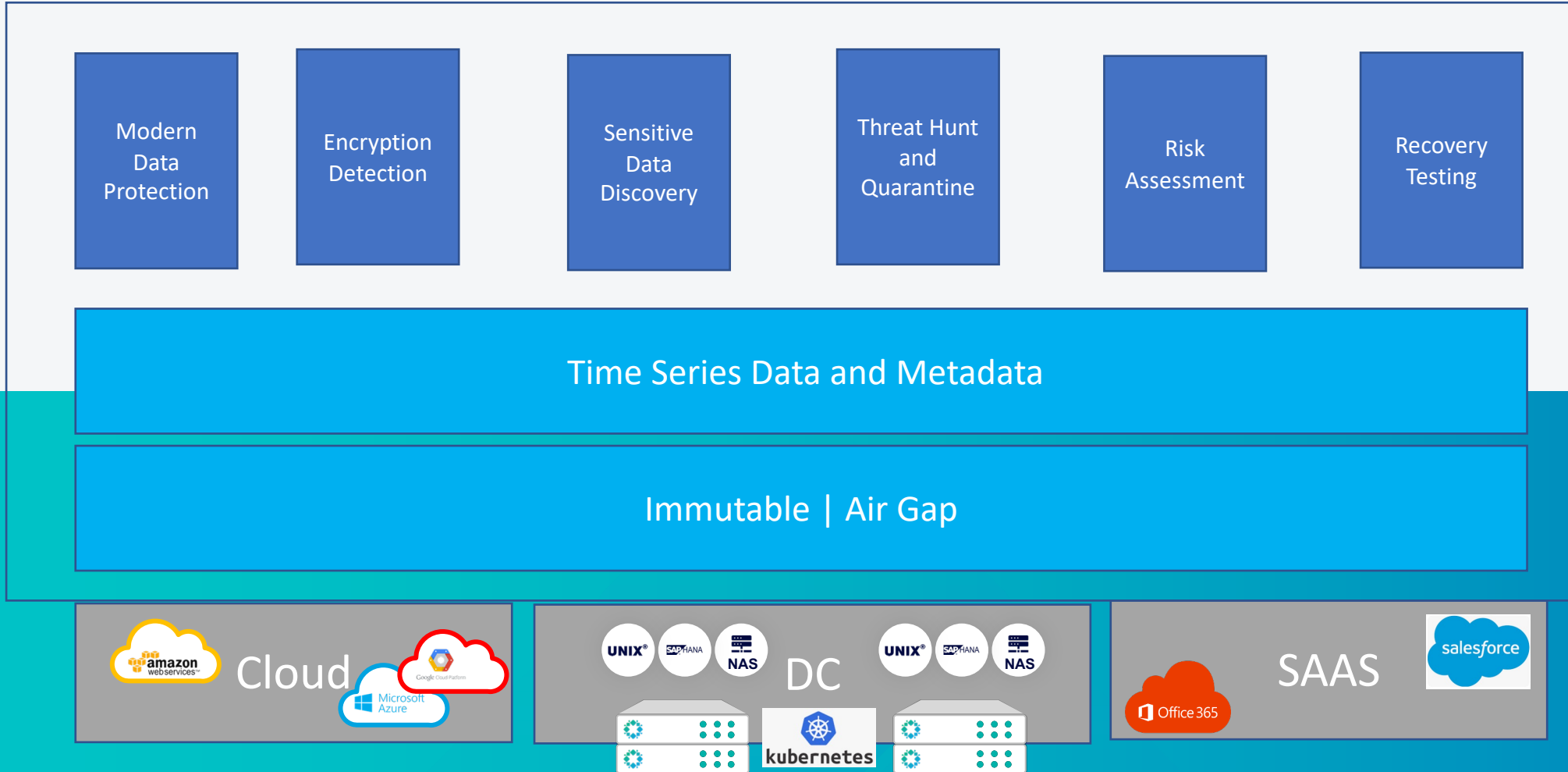
Immutable by Design - so they can't change it

Proprietary append-only file system that doesn't allow changes/modifications



How it Works

Rubrik Security Cloud



Rubrik K8 Backup use cases

- [Disaster Recovery](#)
- Cloud Migration
- Testing (cluster updates, app updates)

5 Kubernetes Security Incidents And What We Can Learn From Them

By Twain Taylor / July 28, 2020

Security continues to be the No. 1 concern for organizations using Kubernetes, and what's interesting is that it has little to do with the inherent unsafety of Kubernetes itself. Instead, it has a lot to do with how complex Kubernetes actually is, and the fact that even skilled cloud-native developers often have a hard time finding their way around. According to a [recent report](#) by StackRox, in addition to a steep learning curve and shortage of skilled labor, exposures due to misconfigurations is the biggest cause for Kubernetes security incidents. After receiving input from over 540 respondents, the conclusion was that over 94 percent had experienced security incidents in the last year!

They were hardly alone, as this short list of major Kubernetes security incidents shows.

Consider pipeline attacks!

Rubrik K8 Architecture Summary

- One protection solution for all your clusters
 - No more backup management on a per-cluster basis
- Off-cluster Backup Control Plane
 - Protection should not be installed on the platform you're protecting
 - Backup agents require minimal cluster resource usage.
- Zero-Trust, Immutable storage.
 - No reliance on cloud archiving for immutable backups.
- Policy defined through Rubrik SLAs
 - No complicated job management
 - Automatically protect any new namespaces in a cluster

```
apiVersion: v1
kind: Service
metadata:
  name: nginx
  labels:
    app: nginx
spec:
  ports:
  - port: 80
    name: web
    clusterIP: None
  selector:
    app: nginx
---
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: web
spec:
  selector:
    matchLabels:
      app: nginx # has to match .spec.template.metadata.labels
  serviceName: "nginx"
  replicas: 3 # by default is 1
  template:
    metadata:
      labels:
        app: nginx # has to match .spec.selector.matchLabels
    spec:
      terminationGracePeriodSeconds: 10
      containers:
      - name: nginx
        image: k8s.gcr.io/nginx-slim:0.8
        ports:
        - containerPort: 80
          name: web
        volumeMounts:
        - name: www
          mountPath: /usr/share/nginx/html
      volumeClaimTemplates:
      - metadata:
          name: www
        spec:
          accessModes: [ "ReadWriteOnce" ]
          storageClassName: "my-storage-class"
          resources:
            requests:
              storage: 1Gi
```


Rubrik Cyber Recovery



**Test Whether Your
Cyber Recovery
Plans Work**

**Recover With
Confidence**



**Clone Data into
Isolated Environments
Faster**

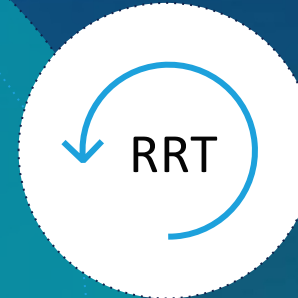
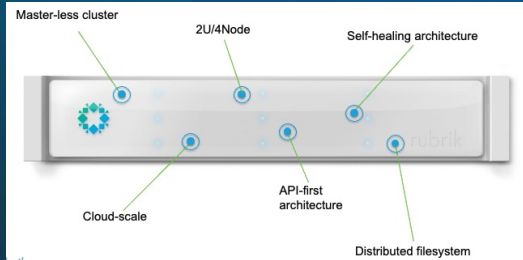
**Perform Security
Assessments Easily**



**Conduct Forensic
Investigations
In Parallel to Recovery**

**Restore Business
Faster**

Zero Trust Architecture



Rapid Recovery Team



5,000+ Customers. 100% Recovered.

FinServ	Manufacturing	Healthcare	Government	Security	Education	Media	Technology	Retail
		AmerisourceBergen			HARVARD LAW SCHOOL	WALT DISNEY		
		NewYork-Presbyterian			Duke UNIVERSITY	SESAME WORKSHOP	facebook	ESTÉE LAUDER
		UCSF Health			UC San Diego	AMERICA'S TEST KITCHEN		
					Imperial College London			SEPHORA
					KING'S College LONDON		DocuSign	
						HEARST		verizon
					UNIVERSITY OF THE PACIFIC			

asså, jag är fan kär i Rubrik.
Helvete vad jag gillar att jobba i
RSC



jag ska ju inte sitta med denna
typen av jobb, men fan, det är
roligt 😊



- Head of IT

Don't Backup. Go **Forward.**

