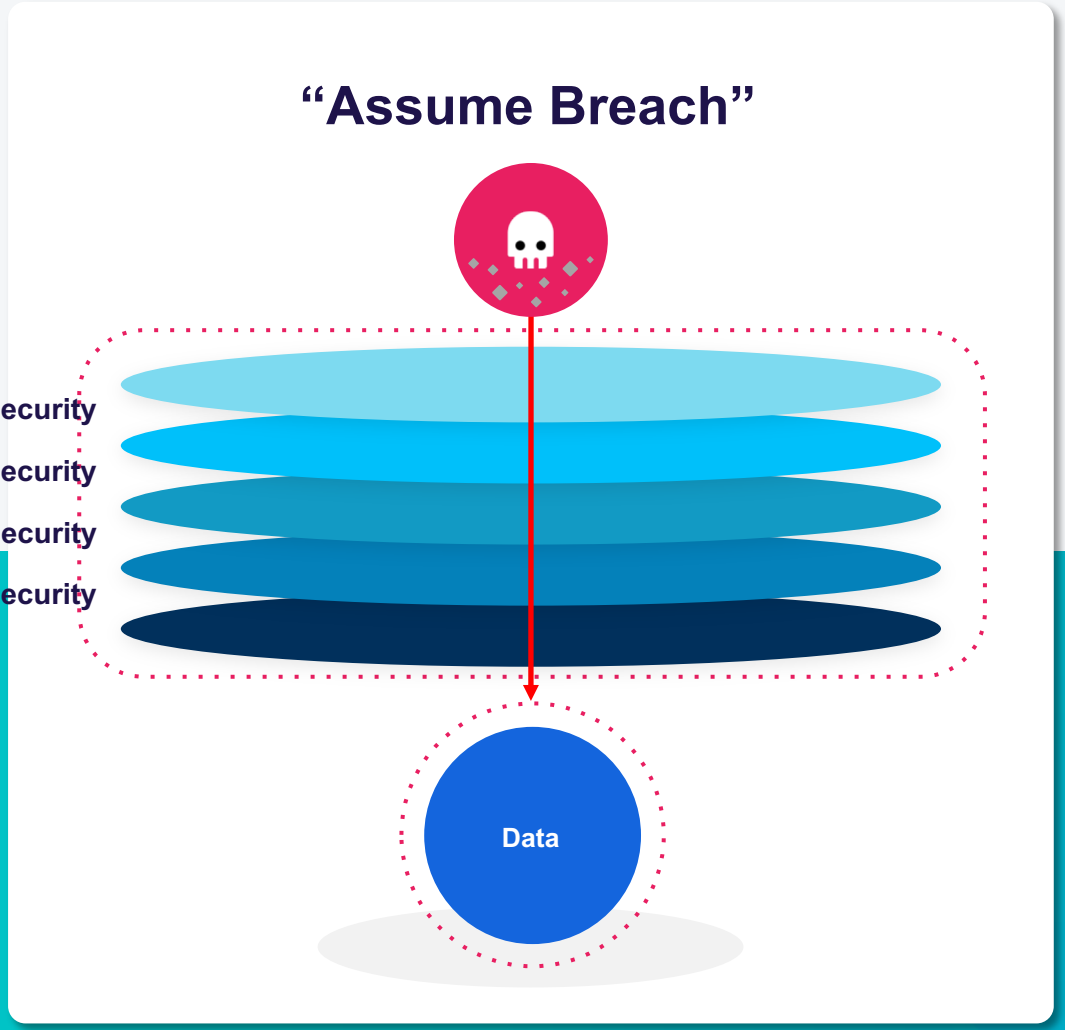
rubrik | Zero Trust Data Security™

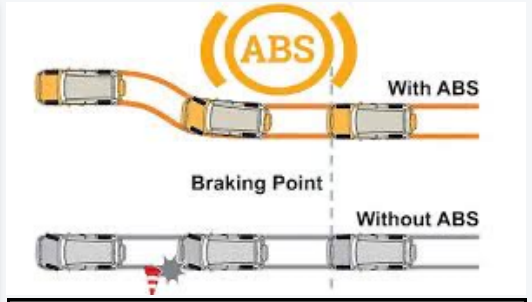
You are under Attack!!!

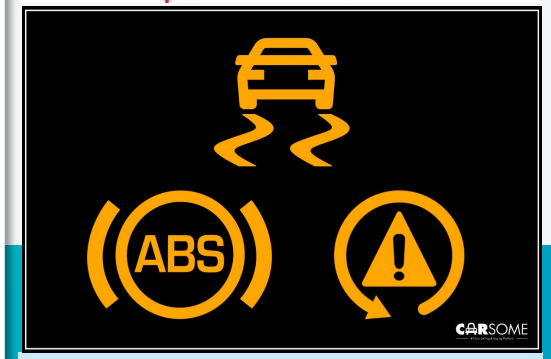
Backup ≠ Cyber Recovery for DC, Cloud, SaaS & K8

Peter Eriksson
Rubrik Architect Nordics

Businesses are under attack & they all have Security







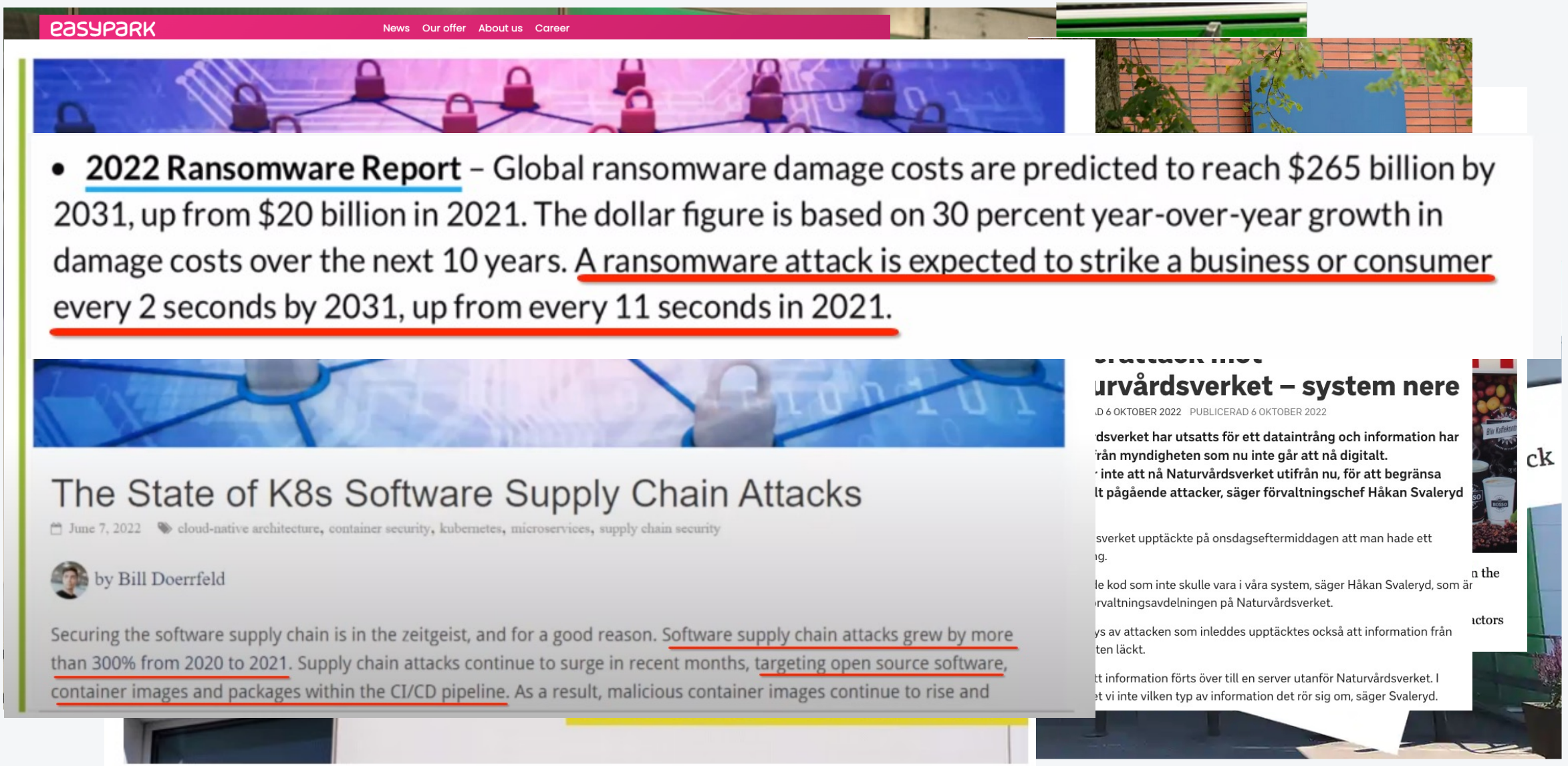
What's your last defence?

PWC CEO Survey

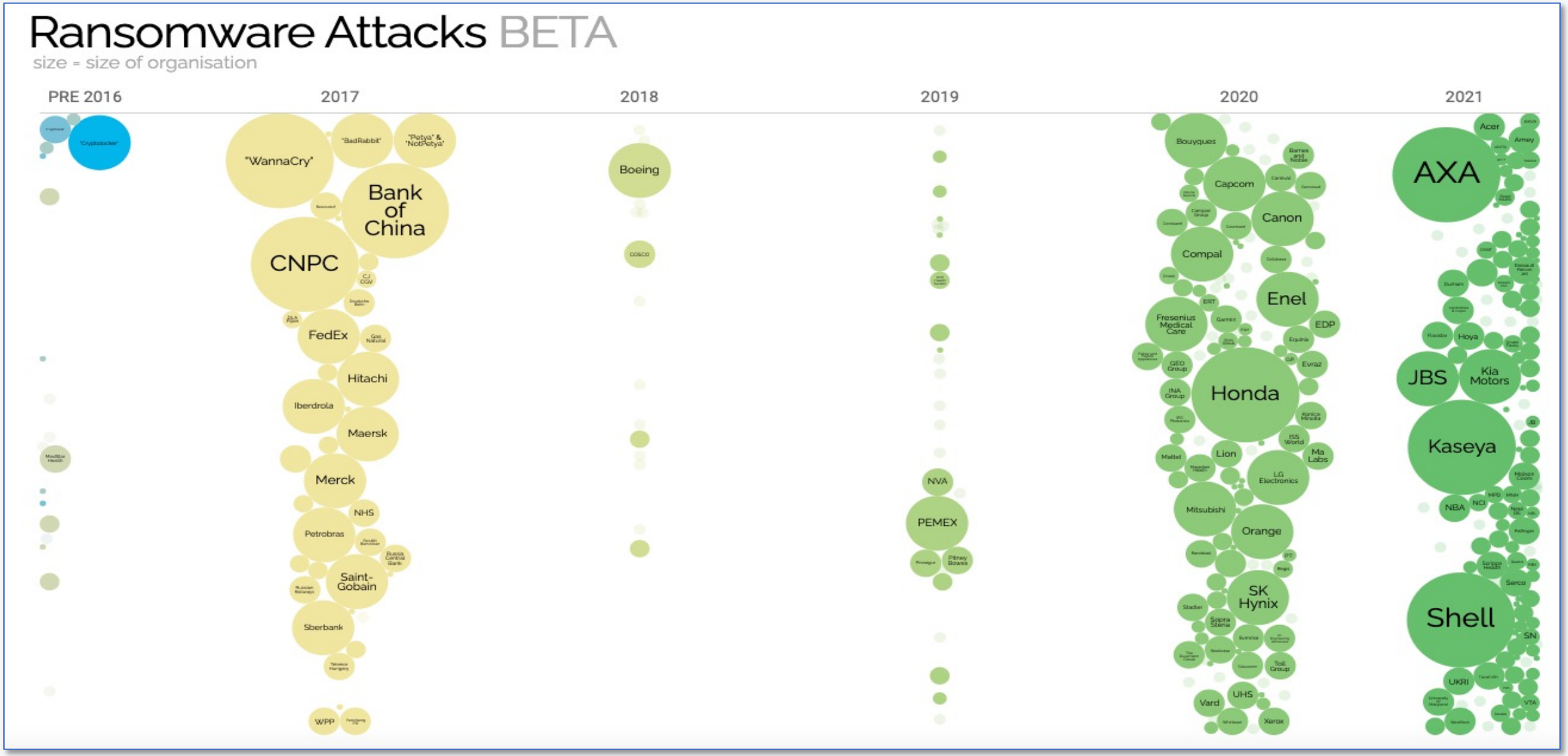
pwc

Enligt ”Cyberbrott mot svenska företag” (2022) av Sevnska 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



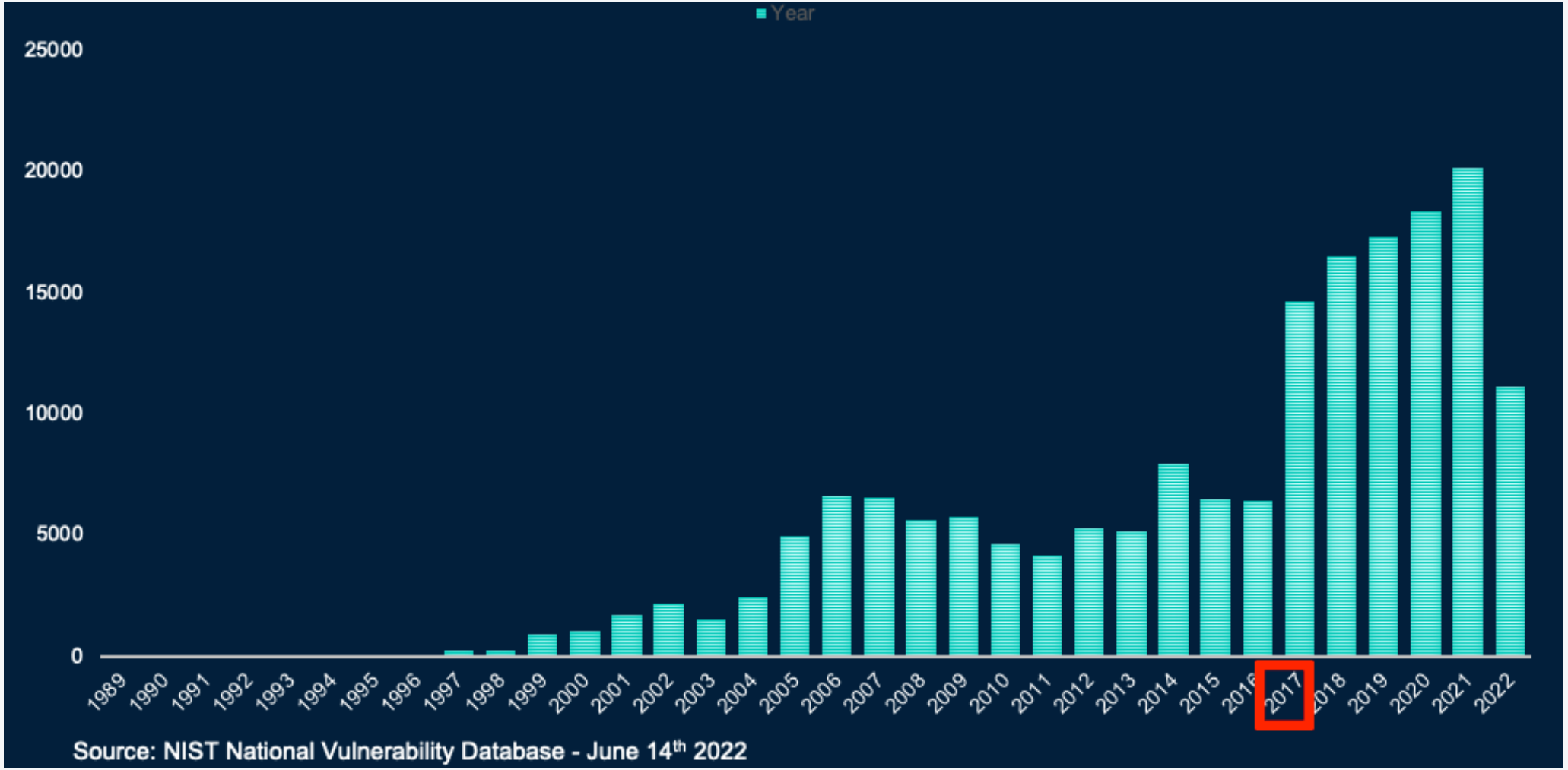
Challenge to keep environment secure- Lots of Patching



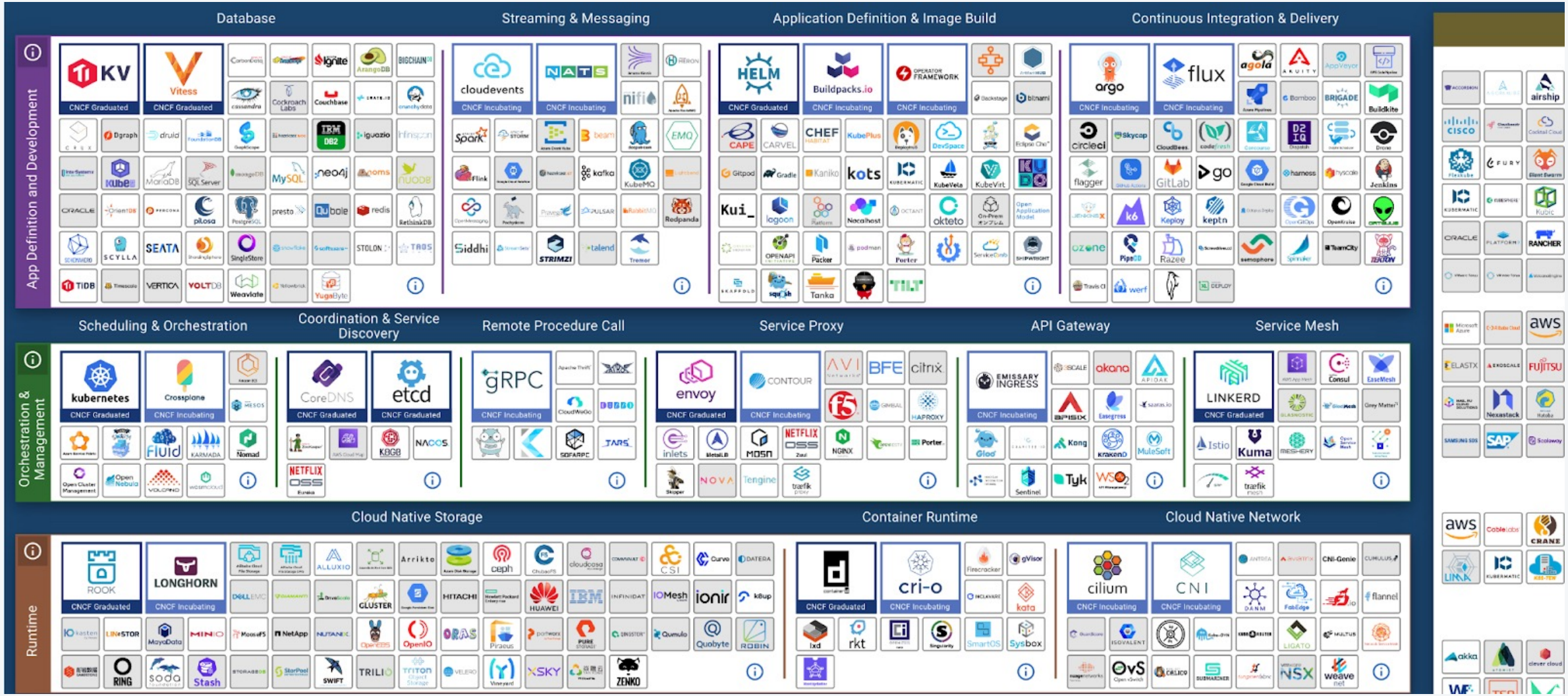
Source: NIST National Vulnerability Database - June 14th 2022 (https://informationisbeautiful.net/visualizations/ransomware-attacks/)

Challenge to keep environment secure

Lots of Patching



Not eaiser in a Cloud Native landscape



rubrik | Zero Trust Data Security™

You are under Attack!!!

Backup ≠ Cyber Recovery

Peter Eriksson
Rubrik Architect Nordics

CYBERSECURITY

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.

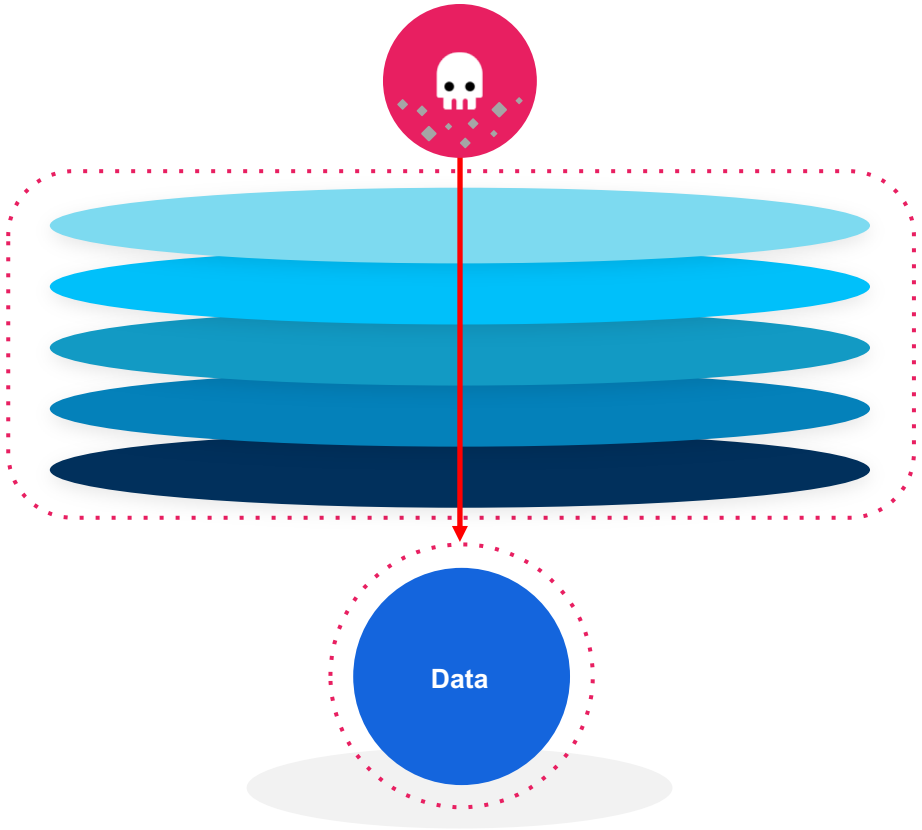
Alex Weinert, vice president and director of identity security at Microsoft, has a favorite quote on zero trust, he said during a recent online panel hosted by Protocol. Weinert once asked a chief information security officer to define zero trust, and the answer he received was, “It means whatever the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

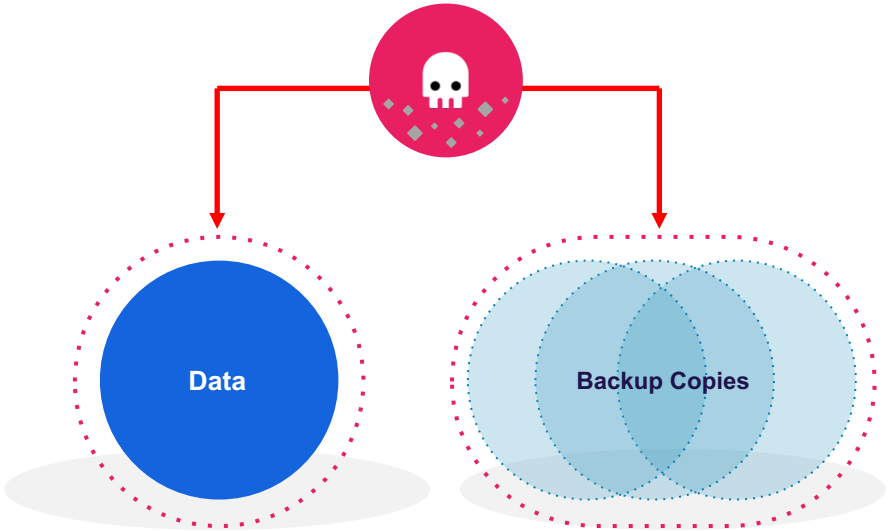
https://www.protocol.com/enterprise/security-zero-trust-cloudflare-zscaler

Businesses are Under Attack

"Assume Breach"



Data and Backup are the targets



CYBERSECURITY

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.

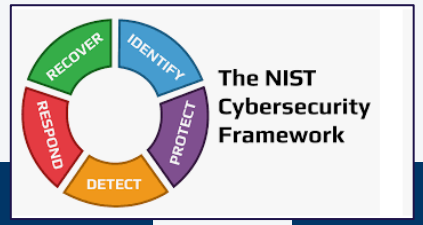
Who can you trust?

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



Infrastructure Security

- Prevention
- Detection
- Investigation

Data Security

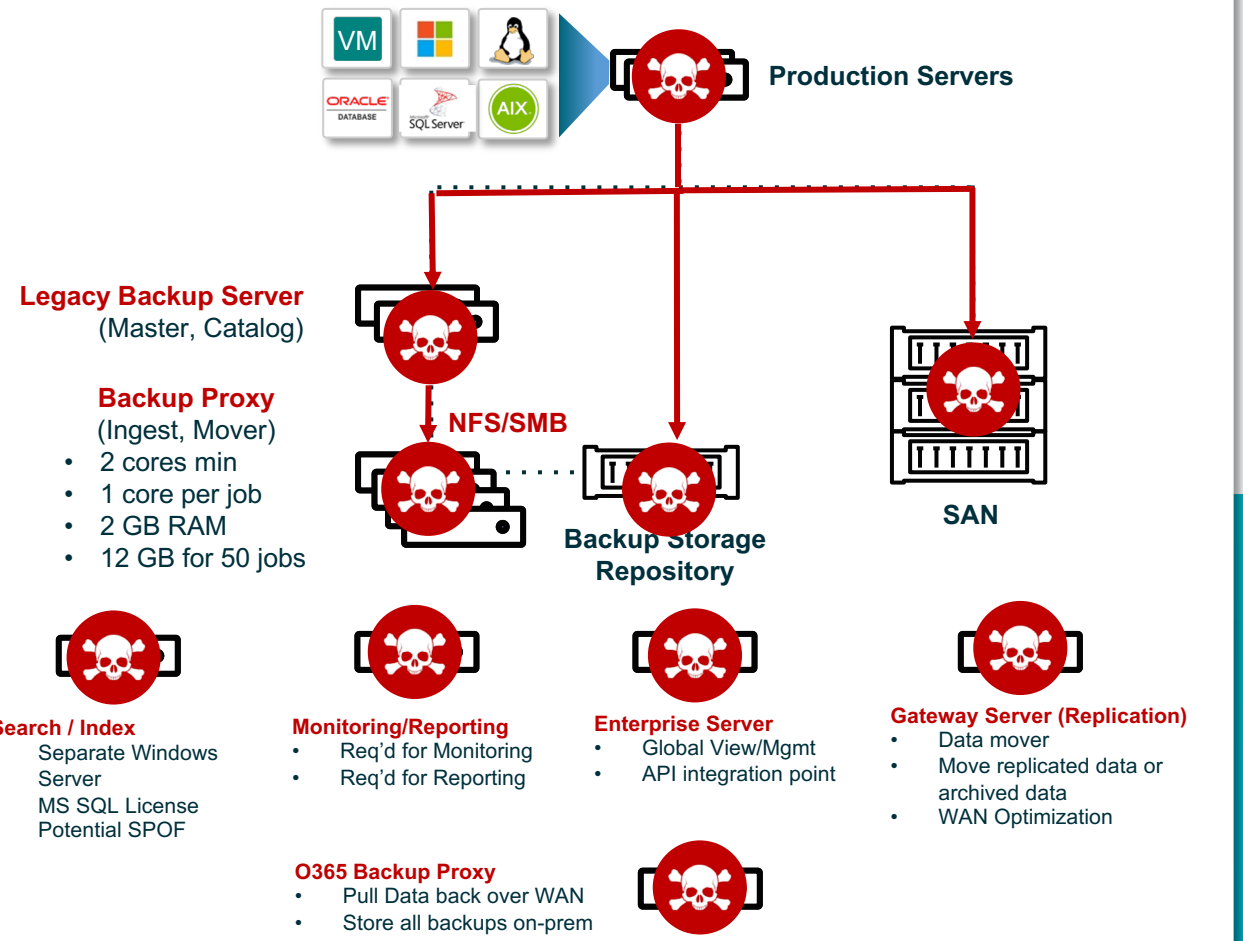
- Data Resilience
- Data Observability
- Data Remediation

Rubrik

Zero Trust Security

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?

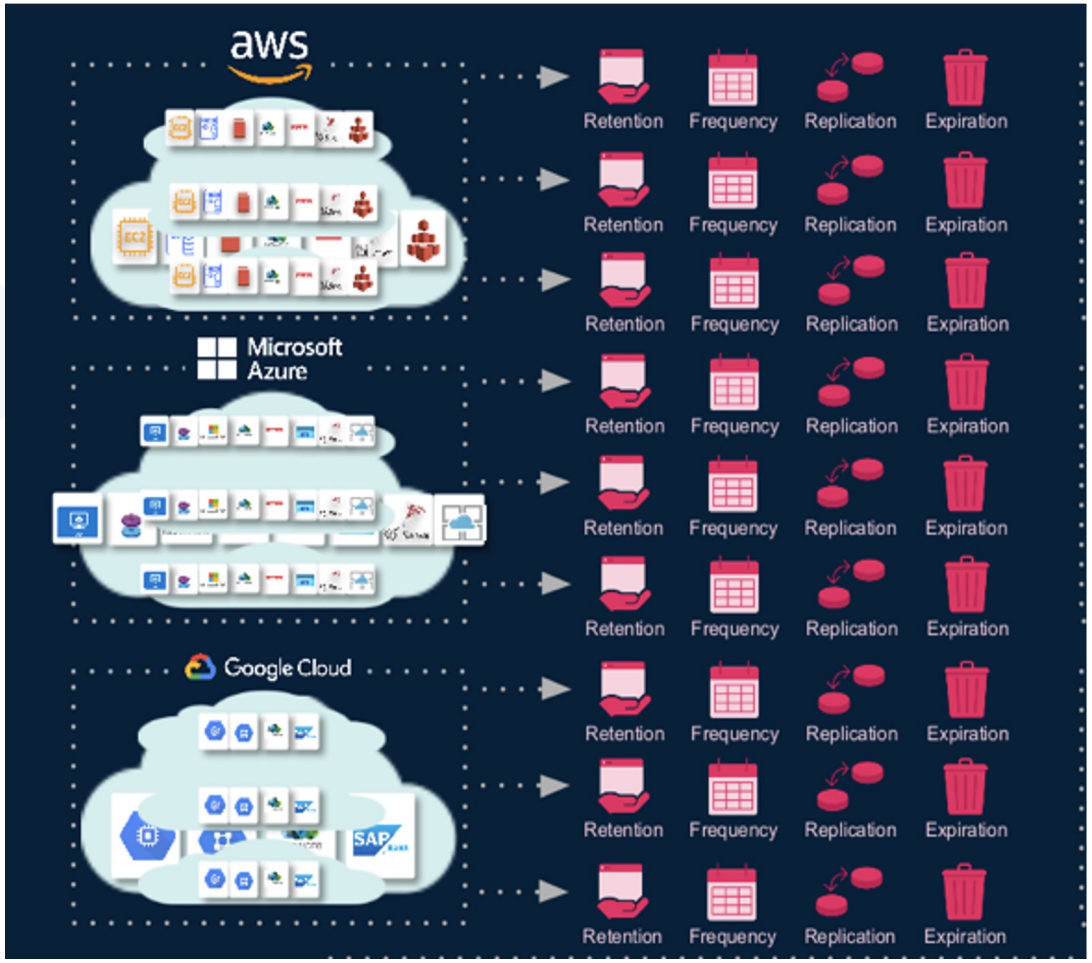


Might not be designed for threats inside your network

- **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?



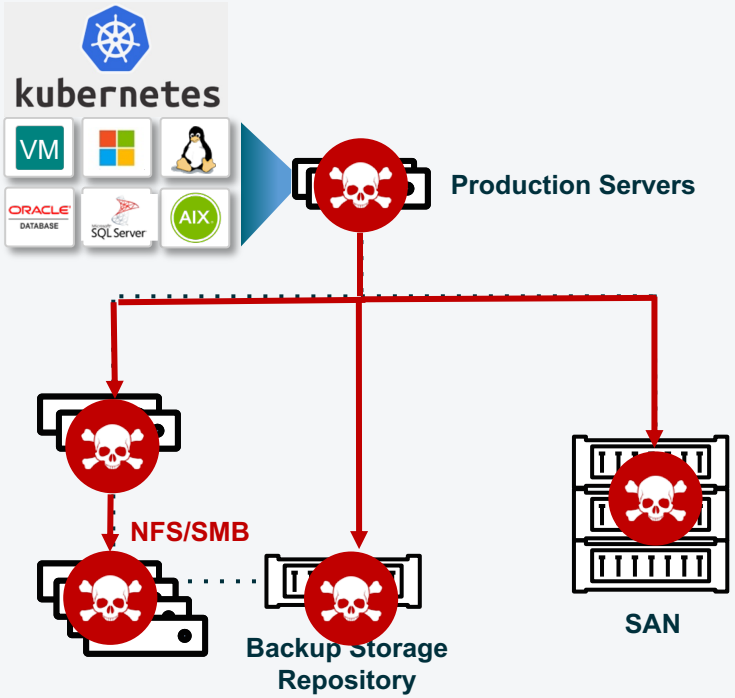
Cloud: New Questions

- 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

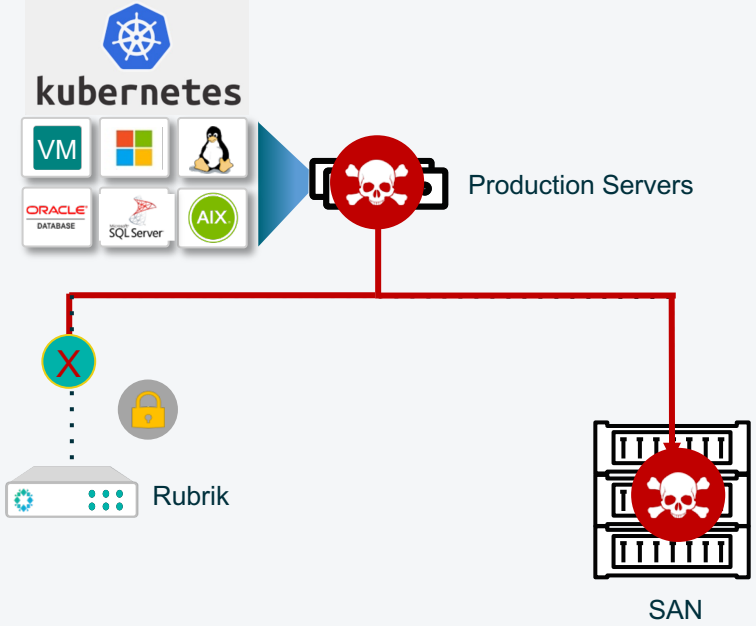
Monitoring/Reporting
- Req'd for Monitoring
- Req'd for Reporting

Enterprise Server
- Global View/Mgmt
- API integration point

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

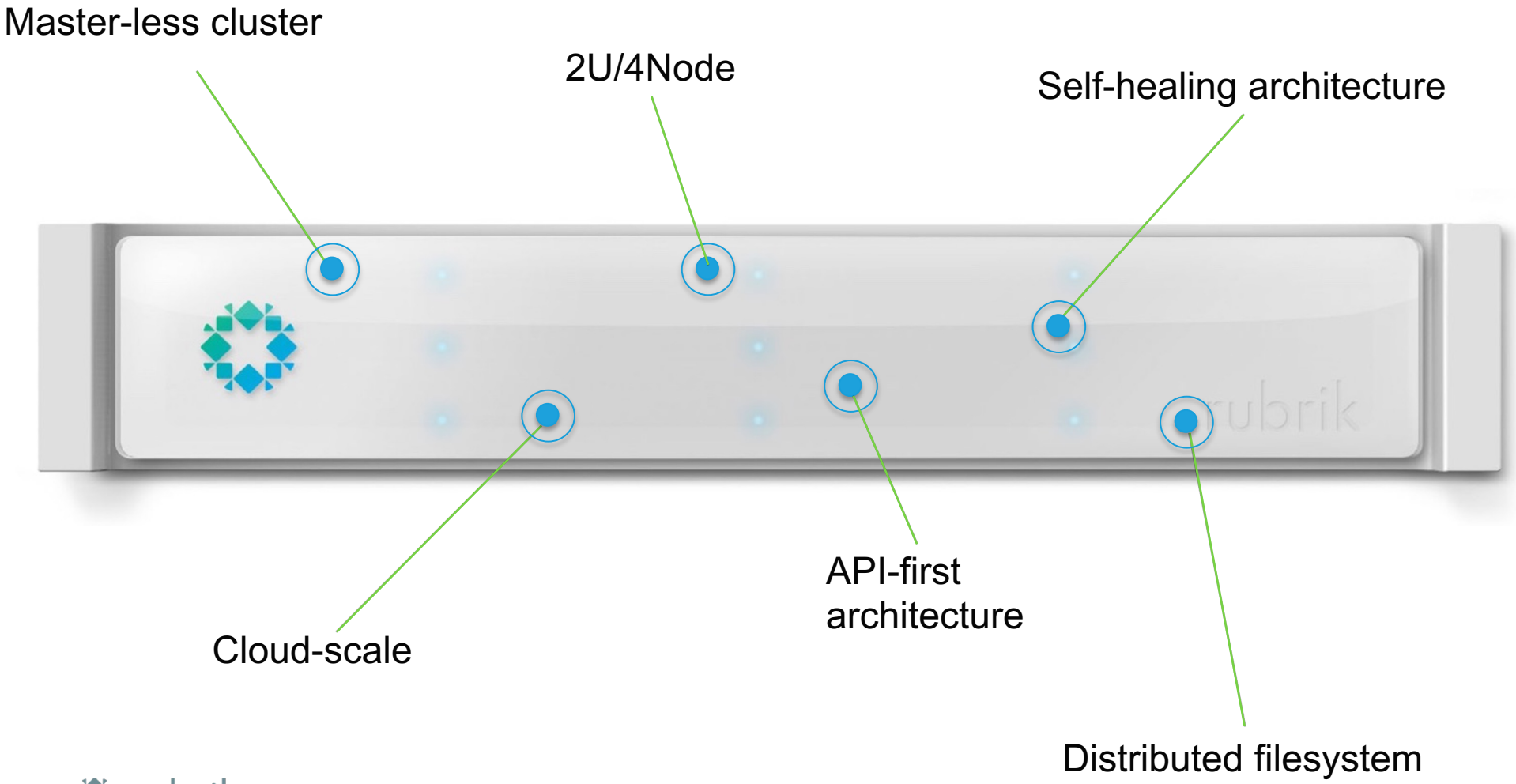
O365 Backup Proxy
- Pull Data back over WAN
- Store all backups on-prem

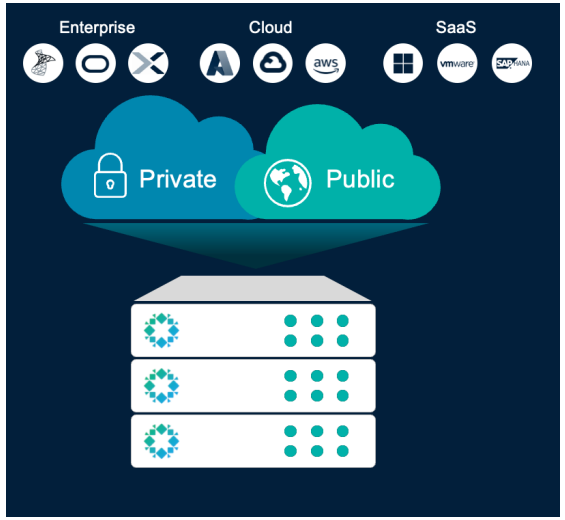
Rubrik Arhchitectural Security - Air Gap



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





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

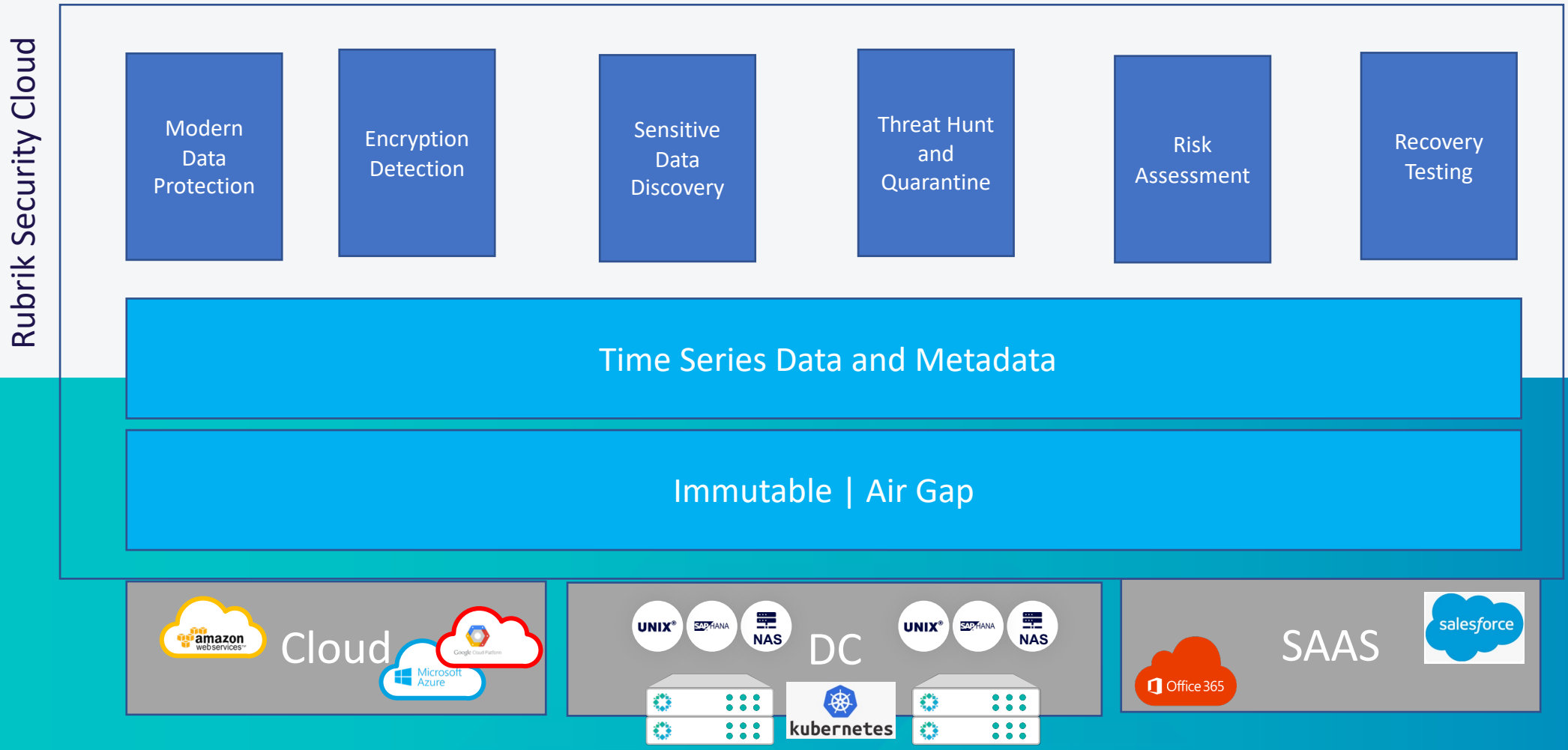
Immutable by Design - so they can't change it

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

rubrik

17

How it Works



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

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

```yaml
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

Rubrik Cyber Recovery

Test Whether Your Cyber Recovery Plans Work

Recover With Confidence

Clone Data into Isolated Environments Faster

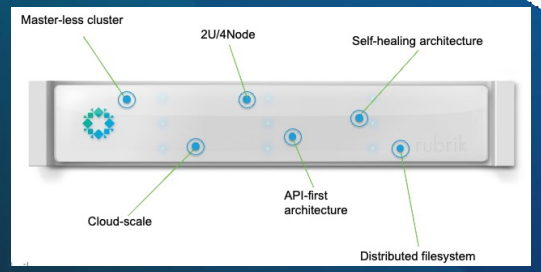
Perform Security Assessments Easily

Conduct Forensic Investigations In Parallel to Recovery

Restore Business Faster

rubrik

Zero Trust Architecture



RANSOMWARE rubrik WARRANTY RECOVERY

RRT

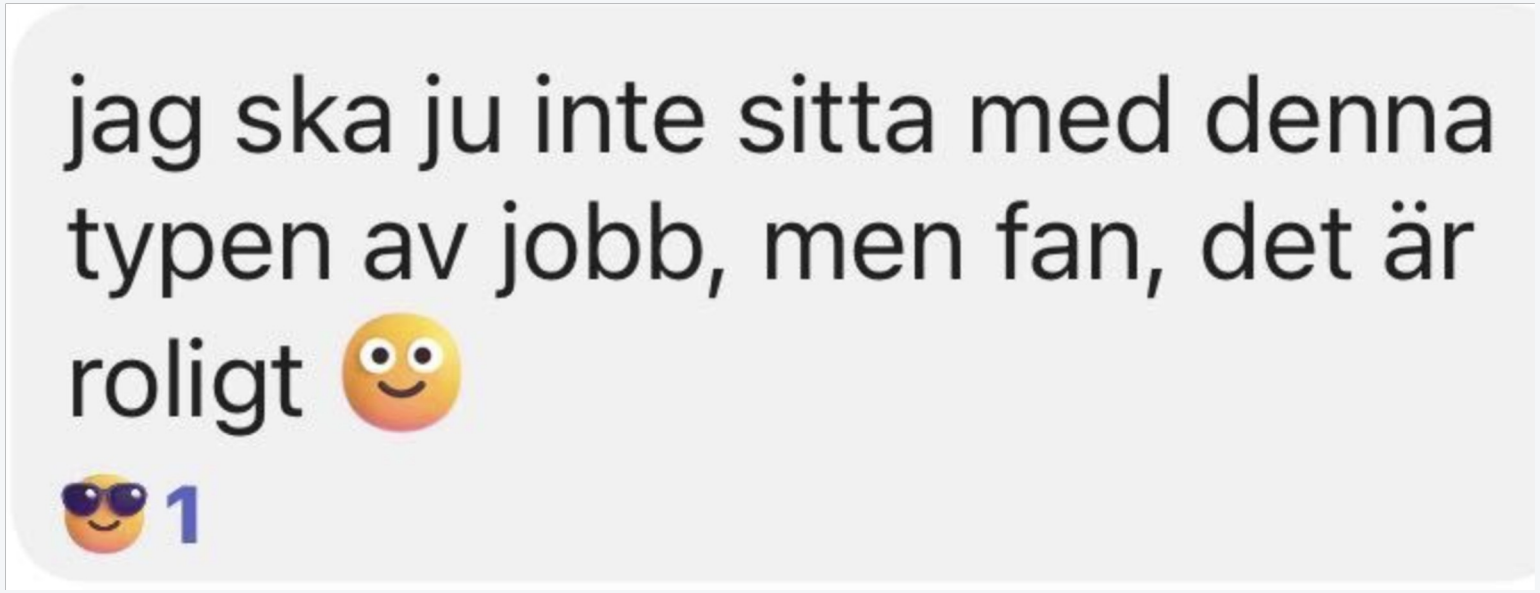
Rapid Recovery Team

Rubrik Zero Labs

rubrik

5,000+ Customers. 100% Recovered.

FinServ	Manufacturing	Healthcare	Government	Security	Education	Media	Technology	Retail
VISA	AMGEN	AmerisourceBergen	IRS	paloalto NETWORKS	HARVARD LAW SCHOOL	Walt Disney		THE HOME DEPOT
Allstate	Kellogg's	NewYork-Presbyterian	FDA	FIREEYE	Duke UNIVERSITY	SESAME WORKSHOP	facebook	ESTĒE LAUDER
MetLife	PACCAR	UCSF Health	CITY OF LAS VEGAS NEVADA	FORTINET	UC San Diego	AMERICA'S TEST KITCHEN	NVIDIA	IKEA
Liberty Mutual	gsk GlaxoSmithKline	Seattle Children's	Scottish Government Riaghaltas na h-Alba gov.scot	SONICWALL	Imperial College London	HBO	Adobe	SEPHORA
USAA	HONDA	DSH	U.S. DEPARTMENT OF HOMELAND SECURITY	proofpoint	KING'S College LONDON	LAMAR	DocuSign	Domino's
CBRE	mazda	Children's Hospital of Philadelphia	Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	imperva	Penn University of Pennsylvania	HEARST	Dropbox	verizon
Aflac	stryker	LEGACY HEALTH	CalEPA California Environmental Protection Agency	tenable	UNIVERSITY OF THE PACIFIC	meredith	cisco	T-Mobile



- **Head of IT**

Don’t Backup. Go Forward.