
DELL Technologies /World
Data Management and Protection in a Transforming World
Kalyan C Gunda
Kalyan.gunda@dell.com

Roadmap Information Disclaimer

- Dell Technologies, inclusive of its seven brands, makes no representation and undertakes no obligations with regard to product planning information, anticipated product characteristics, performance specifications, or anticipated release dates (collectively, “Roadmap Information”).
- Roadmap Information is provided by the Dell Technologies’ brands as an accommodation to the recipient solely for purposes of discussion and without intending to be bound thereby.
- Roadmap information is Restricted Confidential and is provided under the terms, conditions and restrictions defined in the Non-Disclosure Agreements in place between your organization and the brands under the Dell Technologies family.

What's Next?
How will data protection look like in the next decade?

Four IT Mega-Trends on the Horizon

Trend 1: The Data Era Has Arrived

90%
world data created in last 2 years

163ZB
data by 2025

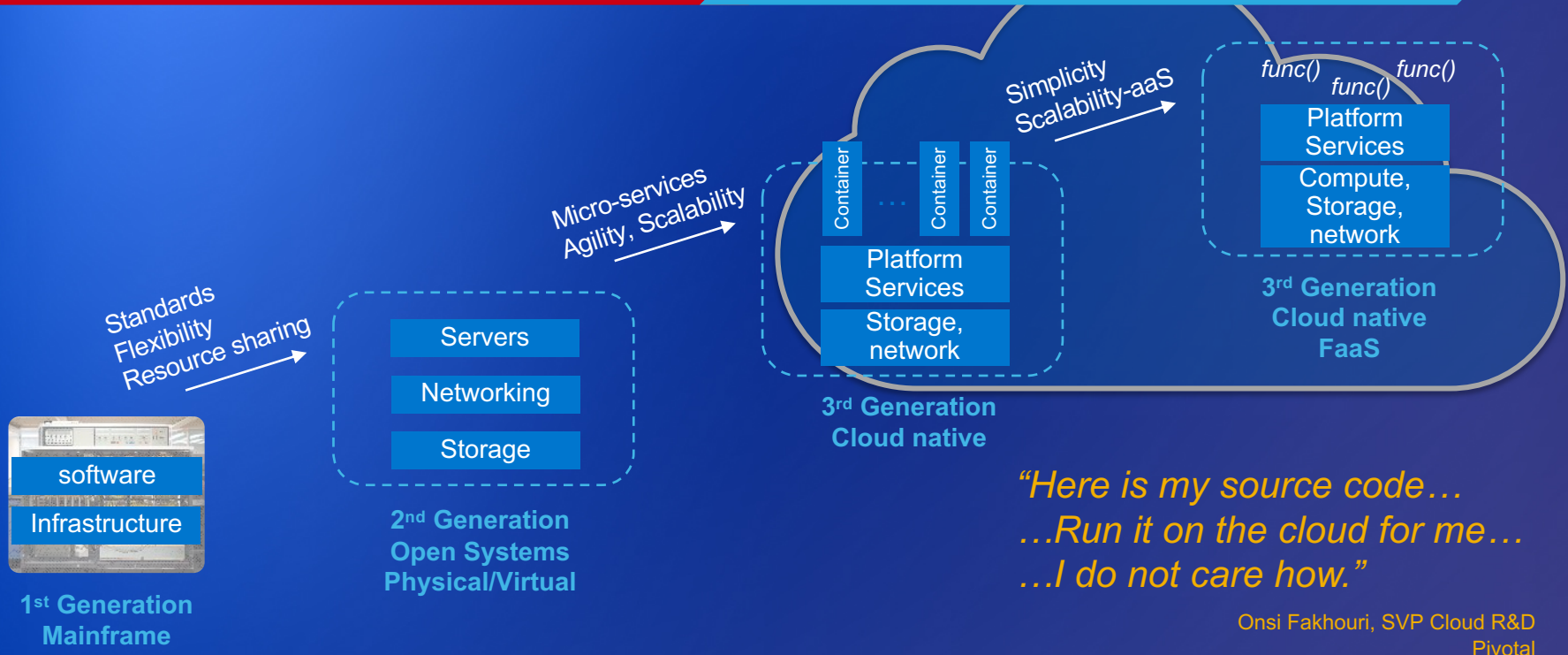
1Q
Yearly files created by 2025

Digital Transformation – Your data IS your business

1ZB = 1,000,000,000,000,000,000,000 bytes = 1,000,000,000 TB

Trend 2: Evolution of Business Applications

Imperative model | Declarative model

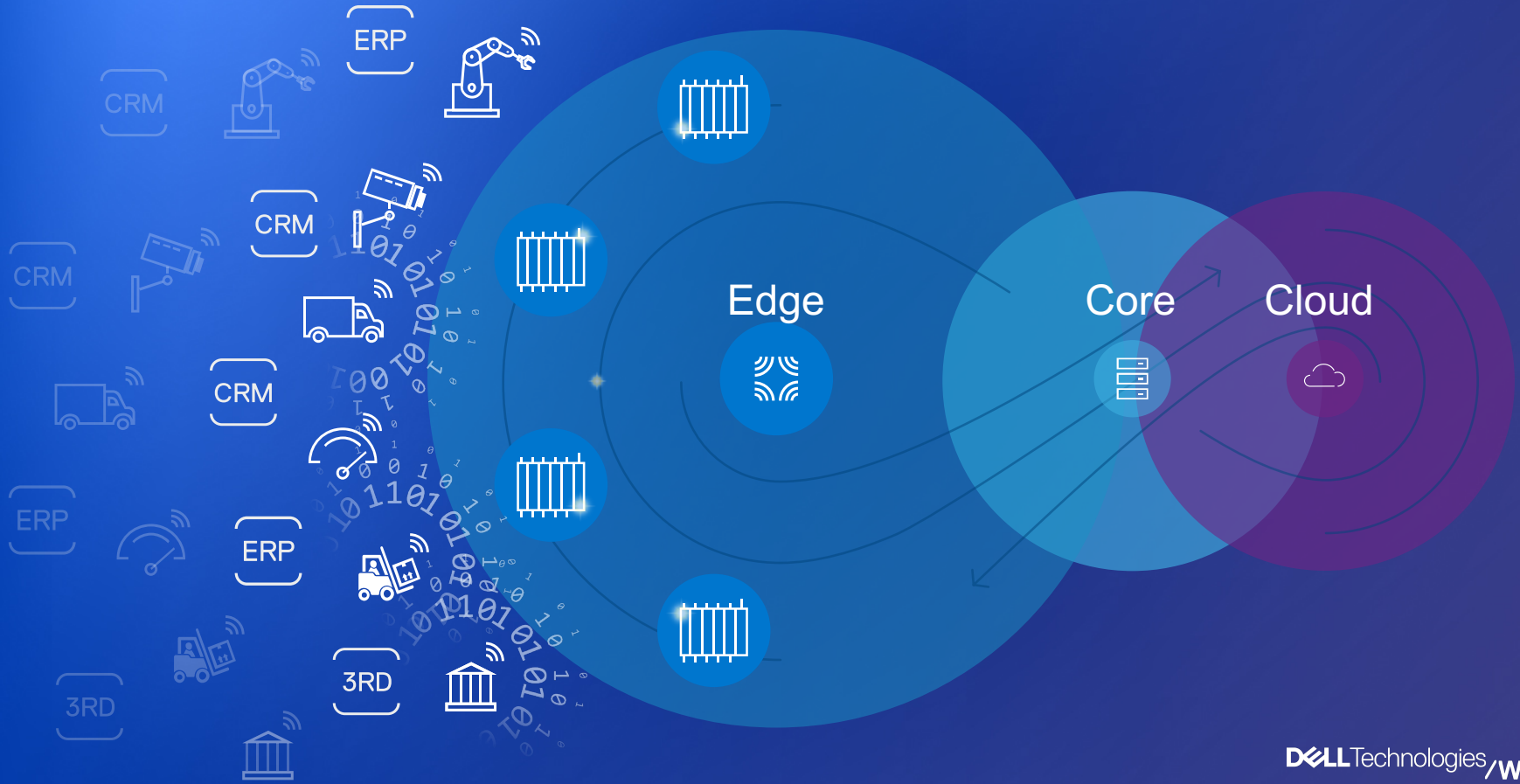


"Here is my source code…
…Run it on the cloud for me…
…I do not care how."

Onsi Fakhouri, SVP Cloud R&D
Pivotal

SW Design: Waterfall | Agile | 12-factor

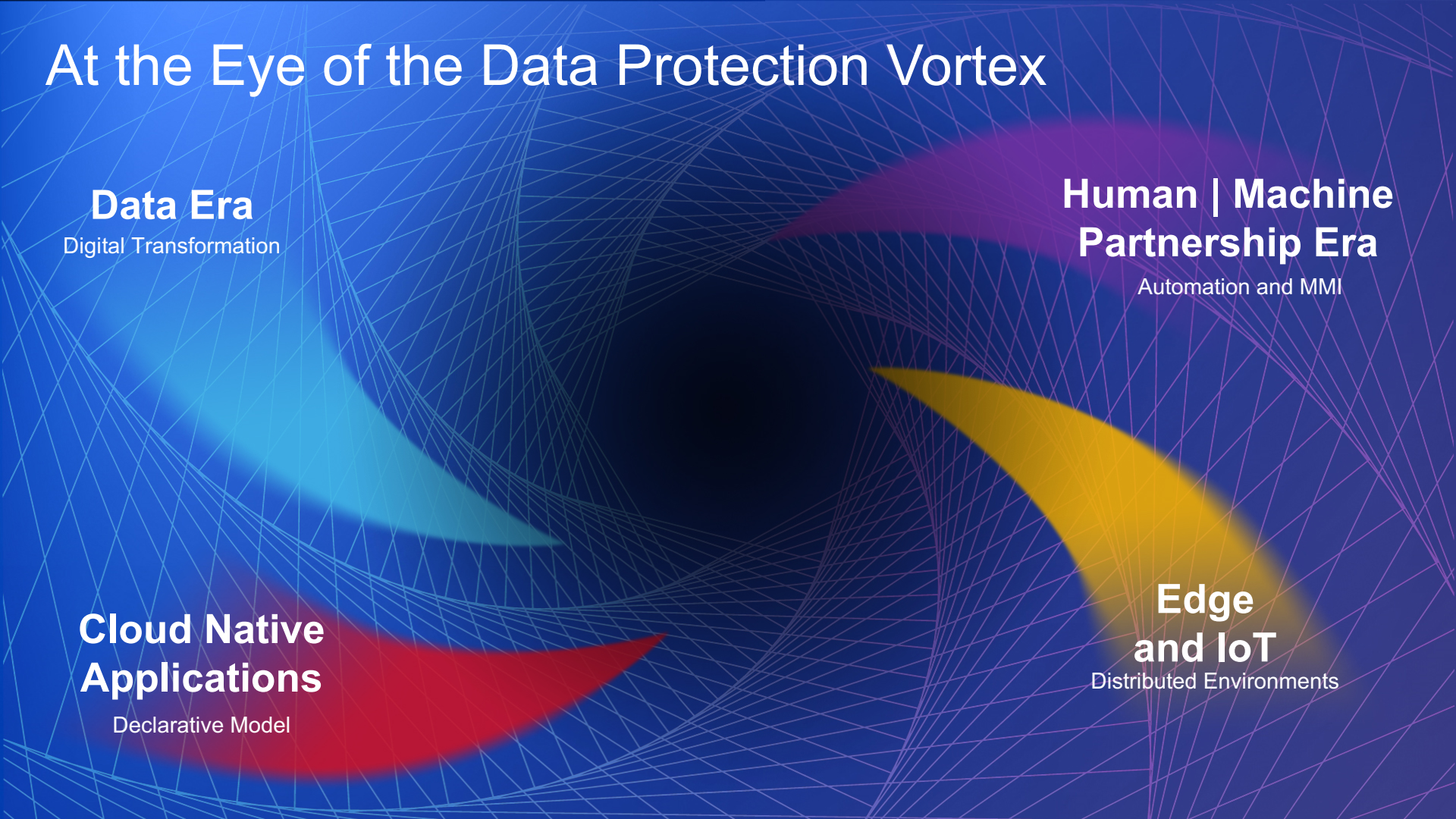
Trend 3: IT Environments Extend to the Edge



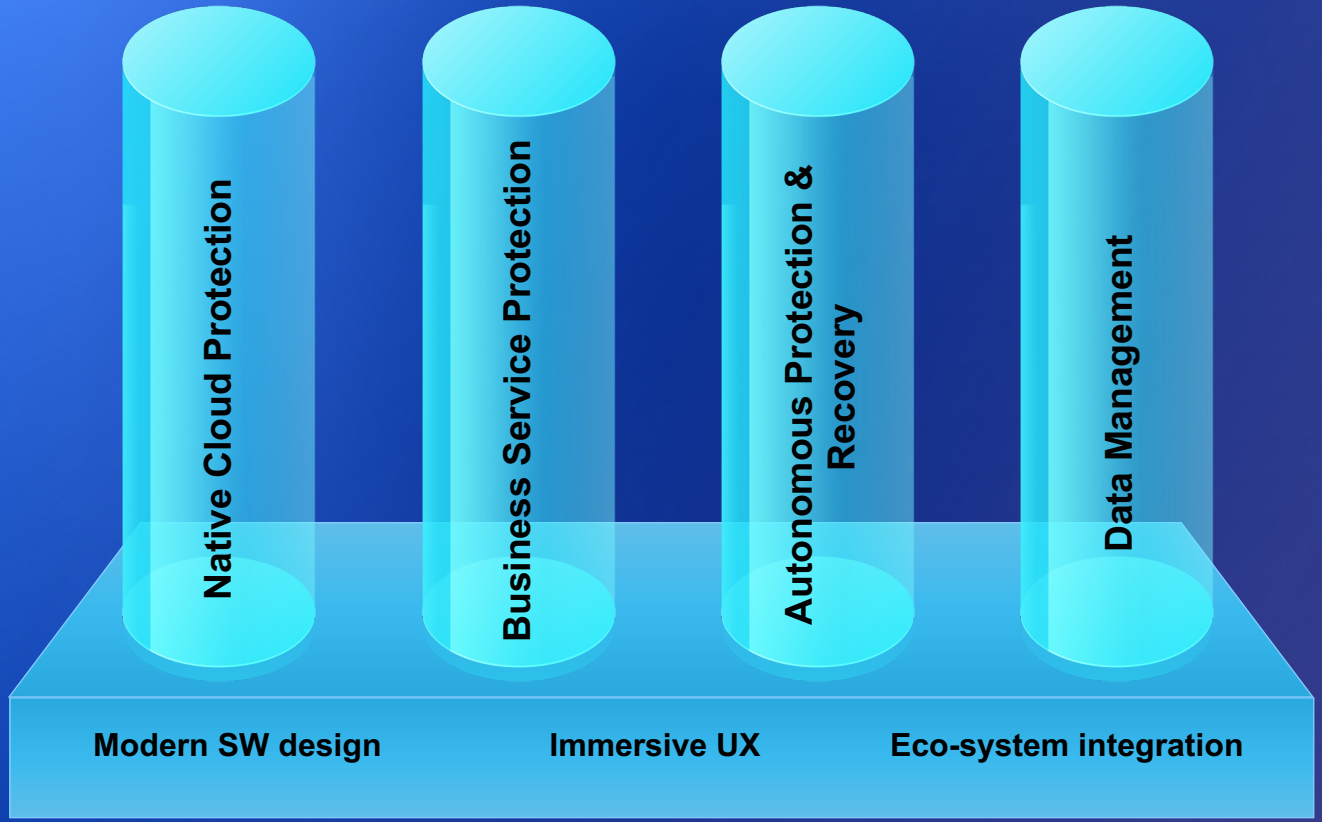
Trend 4: Artificial Intelligence / Machine Learning

The next era of
human|machine
partnerships
and
machine|machine
interaction

At the Eye of the Data Protection Vortex



The Four Pillars of Future Data Protection



1. Native Cloud Protection

- What?
- Where?
- How?

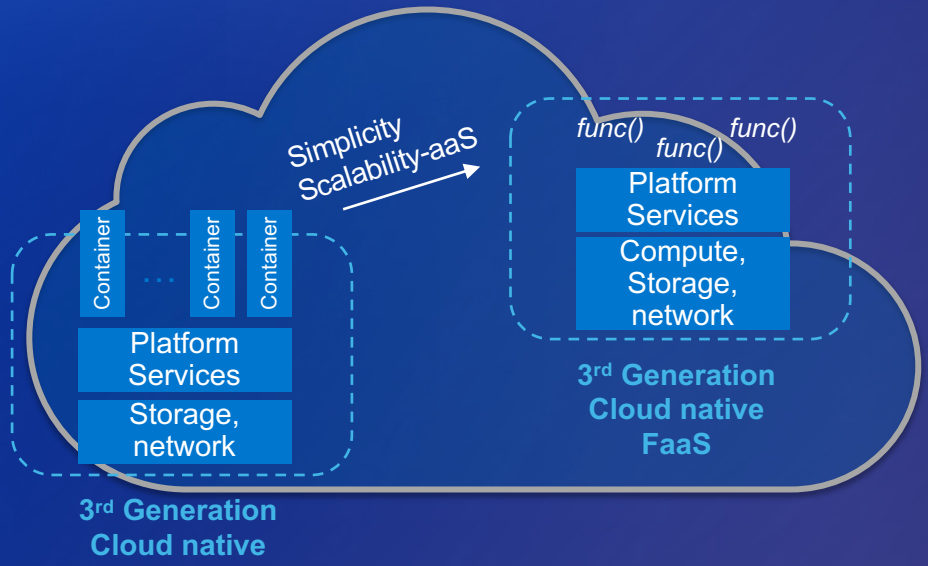
Protecting Cloud Native Applications

1. Protecting persistent data:

- External services
- Within containers

2. Highly dynamic environment, requires high level of automation:

- Integration with cloud native management tools (e.g. Kubernetes manager)
- Integration with DevOps tools (e.g. Ansible)



Protecting the Hybrid-Multi-Cloud

3. Multi-Cloud

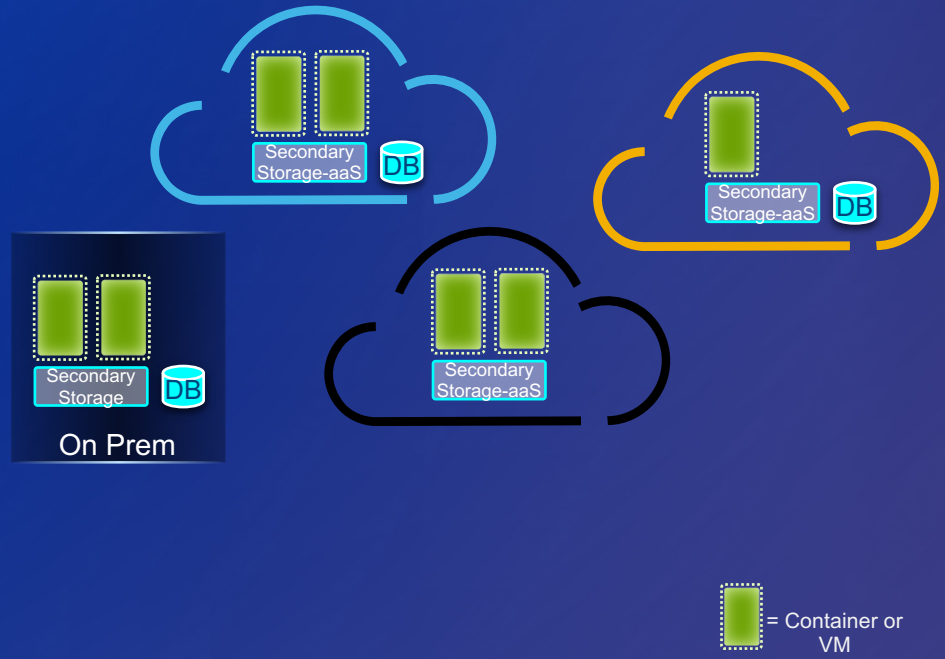
- different apps running on different clouds, requiring:

- SPOG and unified data/assets management

4. Hybrid-Multi-Cloud:

- multiple applications running anywhere, with workload and data mobility, requiring:

- application portable design
- data adaptation
- environment translation
- process automation

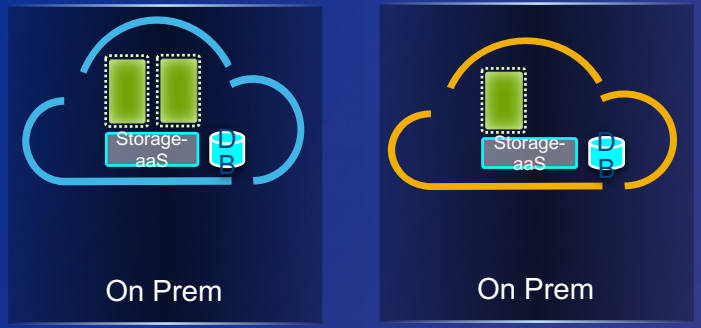


On-Premises Data Center “As A Cloud”

5. On premises data centers will still be around, but…

6. customers expect a “public cloud-like” experience:

- Self-service
- Automation
- Consumption as-a-service
- Software-defined DP
- **“it just works”**

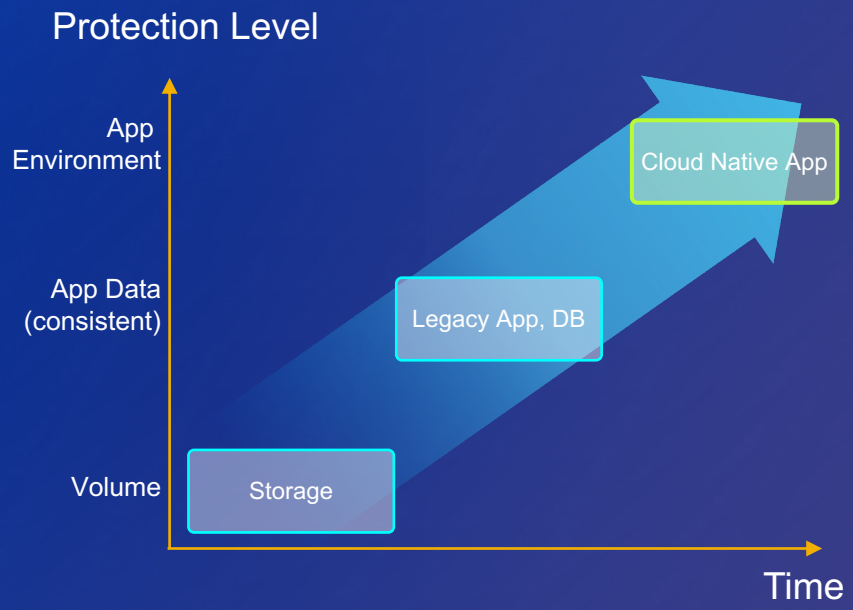


On-prem with cloud-like experience

Business Service Protection

Protecting more than just the data

- **For low/zero RTO, we need to:**
  - Create automation runbooks
  - Test periodically the “recoverability”
  - Simplify decision making process
- **Orchestration should include:**
  - Application/workload recovery, translation, updates (including application metadata)
  - Compute structure (VMs, containers, etc.)
  - Network setting configuration
  - User/application data



3. Autonomous Protection

- Auto-Protection
- Auto-Recovery
- Machine-controlled

Autonomous Business Service Protection

3 Autonomous Protection

1. Automated discovery of application entities:

- Persistent storage in containers
- External services (DB, Files, others)
- App metadata (container images, AMIs, K8S manifests, etc.)
- Image versions (Ansible, etc.)

2. Auto assignment of protection policies:

- Understand data importance
- Historical decisions, other users (“crowd sourcing”), regulation
- Analyze cost and resource implications

Autonomous Business Service Resilience

3 Autonomous Protection

Autonomous recovery without manual intervention

3. Continuous health monitoring:

- Resource utilization
- Environmental indicators
- Data/metadata and application consistency and accuracy

4. Autonomous recovery

5. Phased Introduction:

- Recommendations
- Automatic for less critical apps
- Fully autonomous recovery and validation

Machine-Controlled Protection

Autonomous-Machines will Determine Their Data's Protection and Recovery

3 Autonomous Protection

6. Cloud native applications:

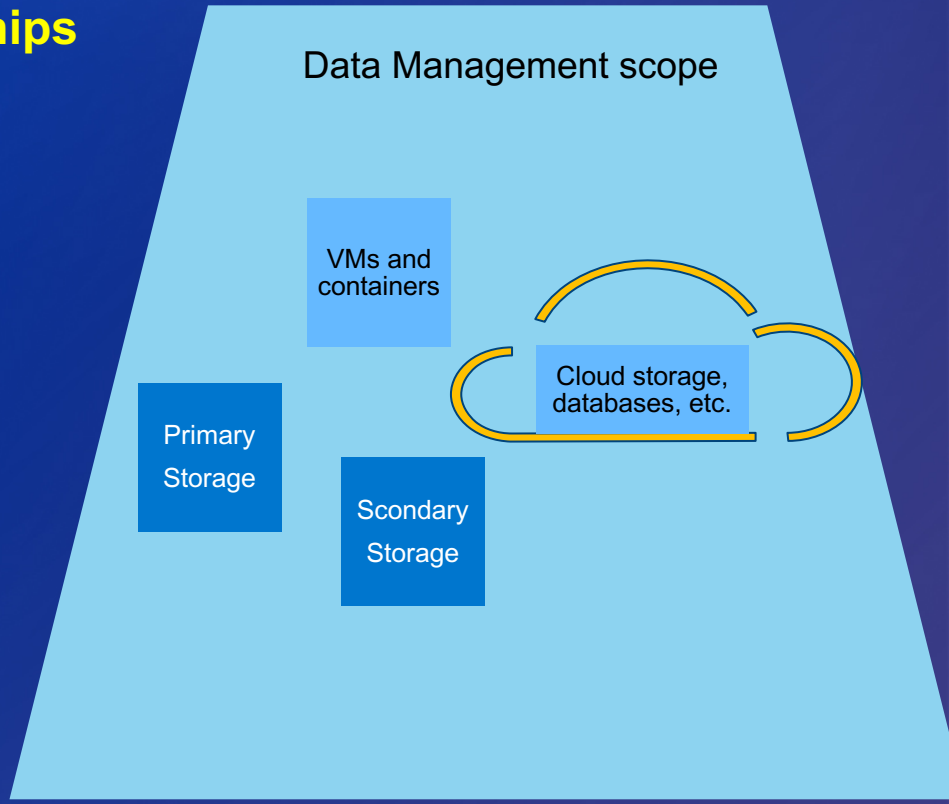
- Dynamic IT environment, high scale
- Cluster/App orchestrators (e.g. Kubernetes Manager)
- DevOps management systems

7. Edge/IoT Compute/devices:

- Local decision on data criticality and protection policy
- Data generation devices
- Edge controllers

Data Life-Cycle Management

1. **Identification of copies and relationships**
2. **Defining copy life cycle based on multiple criteria:**
   - Location
   - Protection level
   - Expiration
   - Meta-data
   - Related application & environment
3. **Metadata analytics:**
   - Data access – warm/cold for tiering, etc.
   - Performance analysis



Data Analytics and Content Analysis

4. Analyzing data and content for:

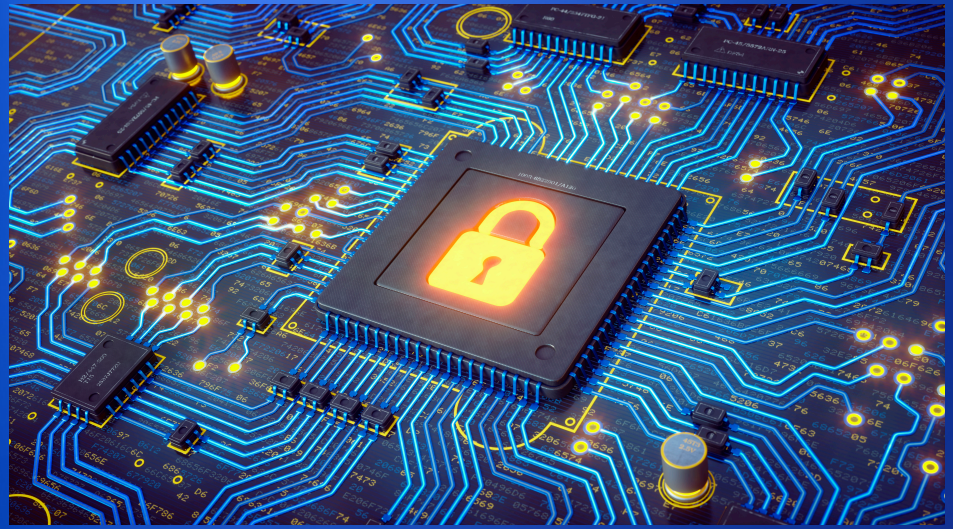
- Protection (criticality; sensitivity, etc.)
- Security
- Policy, governance and regulatory

5. Driving insights for:

- Business growth and optimization
- Improved services and support
- Cost reduction

6. Simplified access (APIs) for external analysis systems

Intrinsic Security



7. Data protection and security are complementary:

- Recovery of previous point-in-time to recover from “data-deletion” attack (e.g. “Ransomware”)
- Proactive measures in case of “data access” attack
- Joint monitoring and analytics of anomalies

8. Interaction through APIs, morphing into an integrated solution

Other Attributes of Business Service Resilience Solutions

Modern design as cloud native applications, enabling:

- Consumption as a service, anywhere in the hybrid-multi-cloud
- Elastic cloud scale, to accommodate variable, high-performance workloads

Other Attributes of Business Service Resilience Solutions

User experience will evolve to be immersive and collaborative:

- From desk computer and mobile device → immersive AR/VR/voice-assisted experience
- Insights and recommendations, not just raw data
- Collaborative with other users (and machines)

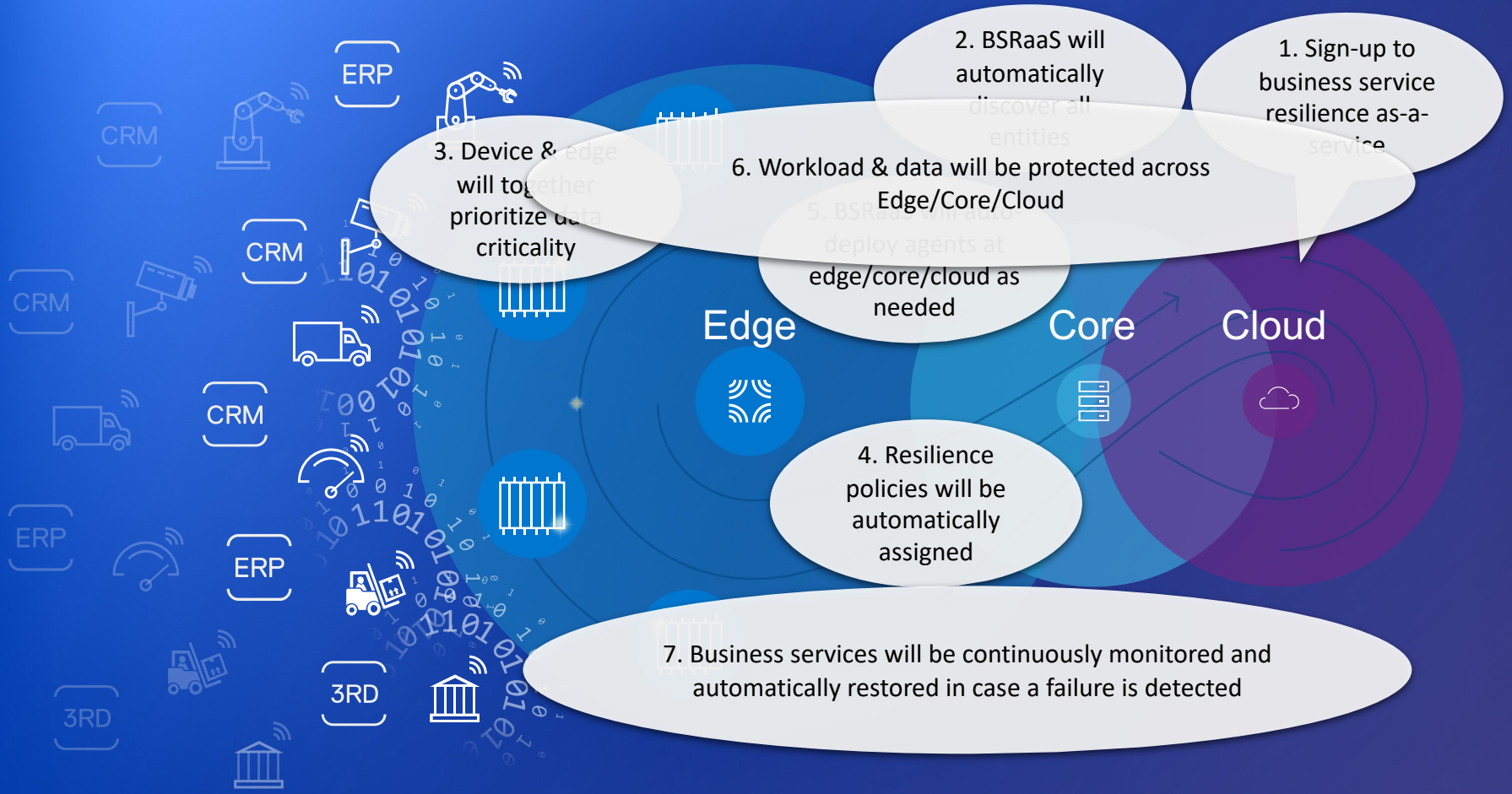
Other Attributes of Business Service Resilience Solutions

Integration with the eco-system – Machine-machine integration:

- API-driven business-resilience as a code

Integrating with:

- **IoT/Edge** services
- **Security** services – to ensure data and workloads are cyber-protected
- **Governance and privacy** services - With inherent privacy and regulatory compliance/governance



“Data-First” Strategy

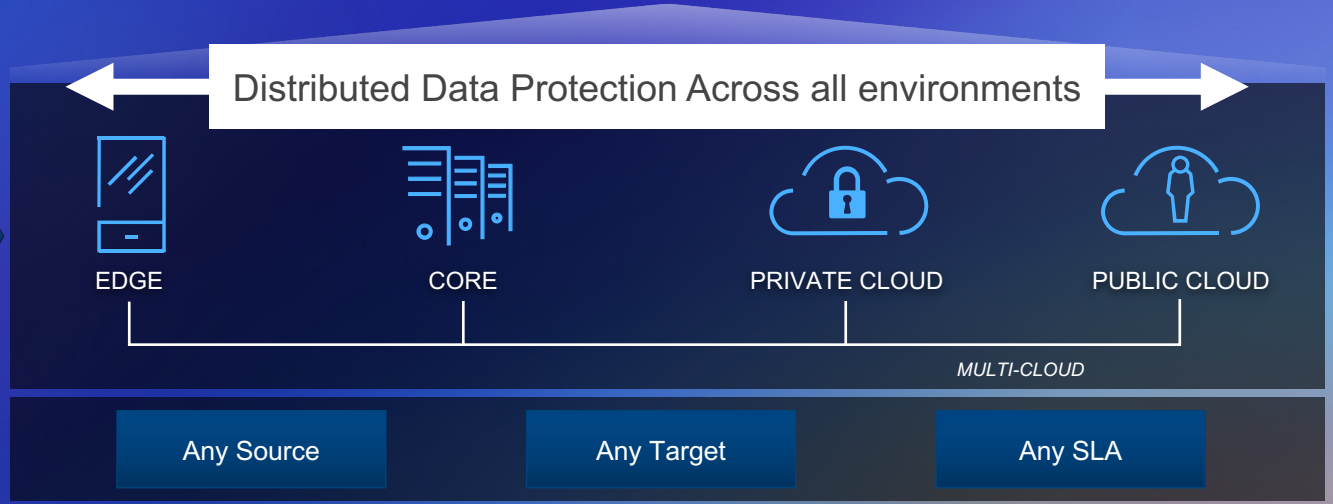
New Business Models

New Data Services

New Consumption Models

Modern SW design

- Software Defined
- Multi-dimensional




DELL Technologies
DELL
DELL EMC
Pivotal
RSA
Secureworks
virtustream
vmware