



TURN DATA INTO ACTION

APPS | CLOUD | IT | OBSERVABILITY | SECURITY



Patented Software No. 7,895,167

Gartner 2015
CoolVendor

Cloud Data Migration | Digital Transformation

Security

Identity | Audit
Access | Forensics

Data driven apps

Business Insights

Operations Intelligence

Compliance & Regulation

API driven Apps

Big Data

AI/ML | Search
Analytics | ODS

DevOps – DevSecOps

Apps Data | Metrics
Performance | Security



Migration to Cloud - Challenges

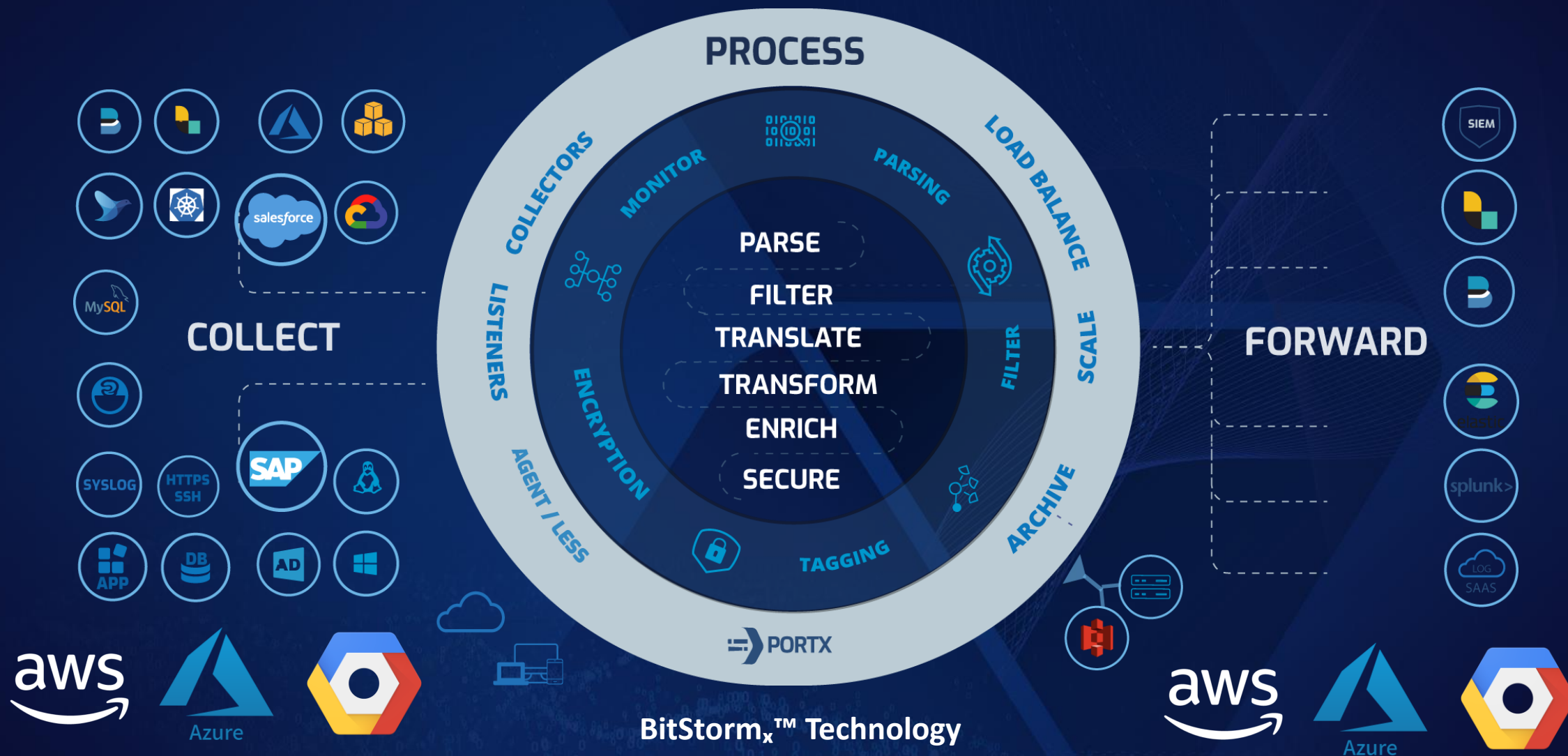
- Speed – Time to Market
- Agility – Changes
- Complexity – Critical data synchronization
- Modern Apps – DevOps | SAAS
- Identity – Security baselines | IDM | P. User | Access
- Security vs. Performance vs. Business Needs
- COST \$\$\$\$ - Efficiency – Cloud is expensive!

Migration to Cloud – Data at Risk

- On – Prem legacy system integration
- Bi – directional data integration – Cloud | Legacy | Cloud
- Identity Control – Data Access | IDM | Audit | P. Users
- 3rd party integrations | SAAS | API
- Complex data needs – Backups, Synch, Access, Speed, Security
- Regulation requirement – time frames | data masking | hashing
- Data Everywhere



Control Data Flows and Pipelines



Biggest Cloud Security Challenges in 2021

According to the 2020 Cloud Security Report by Check Point..



- Highest ranking threat was misconfiguration.
- Potential attack or data leak.
- Unauthorized access, insecure interfaces.
- Account hijacking.
- Complex and ever-changing environments and technologies.

The cloud security controls framework

Move from on-premise to cloud requires a security mindset shift.

Network, platform, and infrastructure

“Security by design” .. zero-trust network security architectures, micro segmentation to allow for varying levels of infrastructure access, microservices, and controls across the network, identity access, and applications.

User and data security

Cloud migration often requires a new approach to data migration and identity. In a distributed system that can be accessed anywhere, user-level access credentials and key management may be required. Identity access management, activity monitoring, reporting, visibility and control are key for security and compliance.

Focus on data protection, privacy, resilience, and regulations, guide data access rights and user privileges.

Data Migration infrastructure and security

Encryption, Access control, speed, flexibility, control, agnostic to cloud providers. Support both on – prem and public cloud data flows and application security needs. Top use cases – compliance, application data, security, backups, regulations, services synchronization, 3rd party integrations.

Core application security

Before moving data or workloads to the cloud, the cloud and cyber teams should determine that the following minimum controls are in place:

- **Data flows and Data Infrastructure planning**
 - Plan data lifecycle and data flows across cloud and edge tiers to determine.
- **Workload protection** for function-based or container-based applications.
- **Secure by design/DevSecOps**
- **Segmentation and zero trust**
- **Audit | Identity | Access** – Ensure identity measures both on on-prem and cloud apps, apply segmentation and security controls into applications architecture.
- **Attack surface management** – manage the vulnerability landscape with tailored services to enhance vulnerability and attack surface programs. Organizations can focus on identifying and assessing cloud assets through their life cycle and across different architecture layers. As an example, smart factories can think through

So...

- Data – Plan the Migration | Security  PORTX
- Identity – Data Access | IDM | Audit | P. Users

Case Study – Cloud (AWS) <> On-Prem (Needs) -

- Digital transformation to the cloud
- Extreme data transfer streaming
- Hybrid – Legacy, Private, Public clouds
- Enable sync | stream between native cloud apps and On-Prem legacy monolithic services.
- KPI's
 - Security
 - Performance – Speed – Efficiency
 - Simplicity
 - Data Integrity
 - Data quality
 - Persistency
- Optimize cost of network and cloud resources.
- Security and UI integration to organization AD.

High performance IT/Cloud data streams

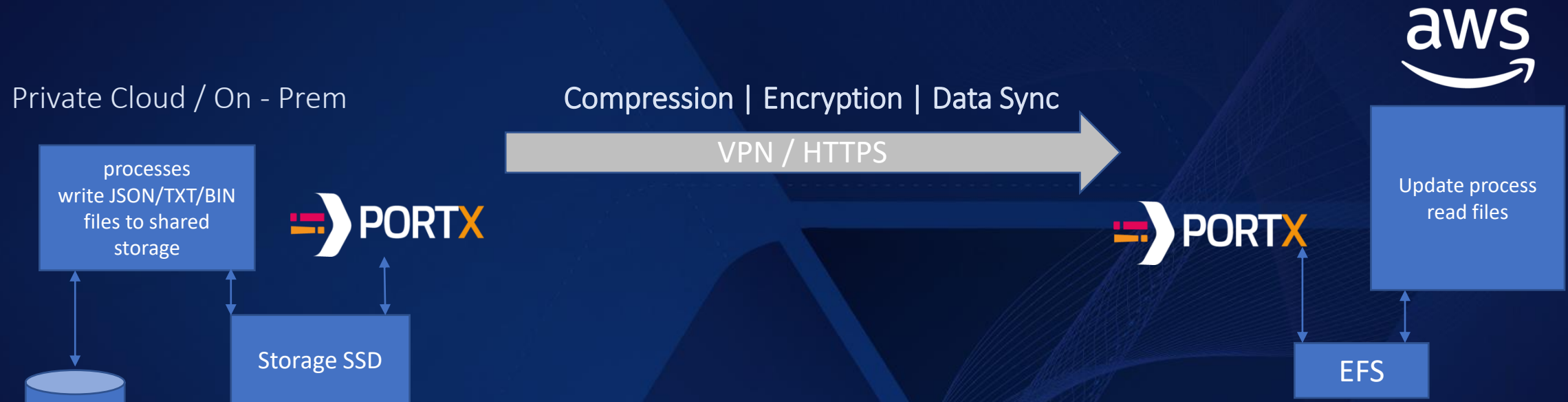
Key Factors -

- Drive data for Apps | API
- Sync Data across IT / Cloud
- Collect | Optimize | Compress
- Route | Filter | Mask
- Live – Real Time sync
- Parse and Enrich data
- UI | Performance | Security

The logo for PORTX, featuring a stylized white and orange arrow pointing right, followed by the word "PORTX" in white and orange capital letters.

BitStorm_x™ Technology

PortX On - Prem & AWS Integration



- Compress and forward only data updates.
- Optimize performance

PortX on AWS sync files to EFS
EFS shared by 3rd party process
High performance
Data update to files synchronously
Data should be streamed – 1st bytes ASAP



- Data center A (On-Prem) EU – AWS East
- Compression – 85%
- JSON – Update files live between business services and cloud apps.
- Network Link to AWS - 100mbit
- AWS Sync Multipart – 5 times slower – does not meet requirements.
- SFTP – 10 time slower – does not meet requirements.

Network 100/100	Total On – Prem <→ AWS PortX	First byte on AWS PortX	Others End to End and First byte: Code AWS MP SFTP
1 file - 100GB	13 min	4 sec	170m 46m 120m
1 file - 70GB	8 min	4 sec	120 min 1500%
1 file – 100MB	4 sec	4 sec	6 min 9000%
1 file – 250MB	6 sec	4 sec	
5 files 100MB + 5 files 250MB	15 sec	4 sec	



Next steps with AWS

Accelerate data migration to AWS

Private Cloud / On - Prem

Agents
Servers
Proxies
Tunnels
Distributed
Any local source



Internal data portals service
sync real time

Everywhere | everyone
Federation | AD security
Elasticity across the grid
Simple – no coding
Security | Compliance | Audit



aws
Marketplace

3rd Party integrations

Data service
RT Streams
Archive
Backups
Security
Analytics
ODS

Streams
Application

Regulation - Compliance

Upload files – synch data:
Salesforce
Azure
Others





TURN DATA INTO ACTION

APPS | CLOUD | IT | OBSERVABILITY | SECURITY

