Multi-cloud Data Security and Privacy for Hyperscale Environment

A conversation with

Srinivas Avasarala
VP, Product Management
SECURITI

Norm Fjeldheim
Former CIO
Illumina and Qualcomm
Moderated by **Mike Meriton**
Co-Founder & COO, EDM Council

- Joined EDM Council full-time 2015 to lead Industry Engagement
- EDM Council Co-Founder & First Chairman (2005-2007)
- Former CEO GoldenSource (2002-2015)
- Former Executive for D&B Software and Oracle
- FinTech Innovation Lab – Executive Mentor (2011 – Present)
Today’s panel

Srinivas Avasarala
VP, Product Management
SECURITI

• Srinivas oversees product strategy and Management at SECURITI
• Previously VP of Product Management for Cloud Security at Symantec
• He has been a part of multiple successful early-stage startups including Palo Alto Networks, Elastica (now Broadcom), and Andiamo (now Cisco)
• Holds multiple US patents and has published in computer networking journals

Norm Fjeldheim
Former CIO
Illumina and Qualcomm

• Norm is the former Chief Information Officer and Head of Global Facilities at Illumina, the global leader in next-generation DNA sequencing
• Prior to joining Illumina, Norm spent 28 years at Qualcomm, the semi-conductor pioneer of 3 generations of mobile wireless technologies
• Norm currently serves on several advisory boards
Every organization has Data Privacy, Security & Compliance requirements

- What personal information do we hold?
- Whose personal data do we hold?
- How is sensitive data currently protected?
- Who has access to sensitive data?
- Where is personal data stored?
- How do we track purpose & legal basis?
- How do we assess data risk?
- How do we monitor data access?
But, business data is spread across Multi-cloud & SaaS

On average, an enterprise has 400+ data assets*

- 80%+ public cloud customers using more than one CSP**
- Drivers for Multi-cloud adoption
  - Access to best-of-breed services.
  - Market driven - serve some specific customers, partners
  - SaaS applications
- Legacy applications in private clouds
- Presents multiple challenges for Data Privacy & Security

* IDC report
** Gartner Research
Data Privacy & Security Challenges Across Diverse Clouds

- Lack of a real-time centralized data asset inventory
- Gaps in sensitive data discovery capabilities
- Handling petabyte scale data volumes
- Scaling manual privacy compliance processes
- Continuous data-centric security posture mgmt. across clouds
Challenge 1: No comprehensive real-time data-asset inventory

- Use of multiple consoles / interfaces separately for each cloud
- Not easy or possible to list data assets across accounts
- Not possible to list data stores that you manage on cloud compute & storage
- Dynamic nature of cloud resources can cause inventory to get stale
Need for a centralized Data Asset Catalog

- That can connect to multiple clouds and accounts
- Run continuous asset discovery
- Discover self-managed data stores too
- Auto-update CMDBs for use in any existing/established downstream workflows/processes
Challenge 2: Gaps in sensitive data discovery capabilities

- Fragmented approaches across clouds provide inconsistent results

- Weak coverage across a broad array of personal and sensitive data elements

- Detection schemes using basic pattern matching techniques have poor accuracy.
Need for a higher efficacy data discovery approach

- With a unified detection engine that provides consistent results across all data
- Has comprehensive coverage spanning both privacy and security for multiple verticals
- Provides more accurate detections using contextual analysis, advanced techniques that leverage file type, and also NLP/ML algorithms
Challenge 3: Handling petabyte scale data volumes

- Object stores use has grown beyond traditional data protection use-cases, and into microservices based apps & data lake architectures
- Modern cloud data warehouses scale to PBs for time-series, logs, ML, and other use-cases
- Traditional Data Discovery tools aren’t suitable for cloud data stores
- Data residency and high transfer costs dictate that data not be moved
Need for a scalable data scanning architecture

- Scanning engines should be elastic based on your data volume as well as your scan time expectations
- Run in customer accounts/premises
- Have the ability to flexibly scope data scans to specific targets of interest
- Use configurable scan optimization techniques
- Support for big data formats like AVRO, Parquet, etc.
Challenge 4: Maturing manual privacy compliance processes

- Survey driven approaches to Data mapping have inaccurate/stale Records of Processing Activities

- No easy way to determine identity information for personal data stored in cloud; this is a must to serve DSARs

- Managing and honoring user’s consent across a variety of data systems
Need for PrivacyOps Automation

• Dynamically update your Data Maps with new data based on Data Discovery

• Trigger new assessments in real-time and update your risk register based

• Correlation of personal data across data systems to specific identities

• Configurable workflows allow dynamic sync of consent status across a variety of data systems/apps.
Challenge 5: Continuous data-centric security posture & access mgmt.

- Cloud security posture tools manage resource misconfigurations (encryption, public access, etc), but without a sensitive data perspective

- Enforcing sensitive data access controls in cloud data lakes/warehouses requires manual tagging of tables and columns

- No centralized compliance view for workloads that span clouds
Need for a centralized Data Security

- Continuous checks for security misconfigurations
- Automated remediation of misconfigured security settings
- Mapping checks to standard controls for compliance reporting - CIS, PCI, SOC2, etc.
AI Powered Data Privacy & Security
across multi-cloud, SaaS and on-premises
Awards

**WINNER
"Most Innovative Startup" RSAC 2020**

Forrester Wave
**LEADER in Privacy Management**

**WINNER
"HPE-IAPP Innovation Award" 2020**

**WINNER
"Top 10 Coolest Security Companies 2020" CRN**

**WINNER
"Most Innovative" Frost & Sullivan**

**FORBES
Top 10 Cyber-security Startups 2020**
Additional Resources

Cloud Data Management Capability

AI Powered
Data Securiti & Privacy
across Multi-Cloud, SaaS and On-Premise

Request demo

BLOG
Sensitive Data Intelligence
Driven Privacy and Protection

WHITEPAPER
Secure Cloud
Data Migration

Download Now

Key Considerations for
Secure Cloud Data Migration
Questions?
FOR MORE INFORMATION:

Srinivas Avasarala
VP Products
Securiti
srinivas.avasarala@securiti.ai