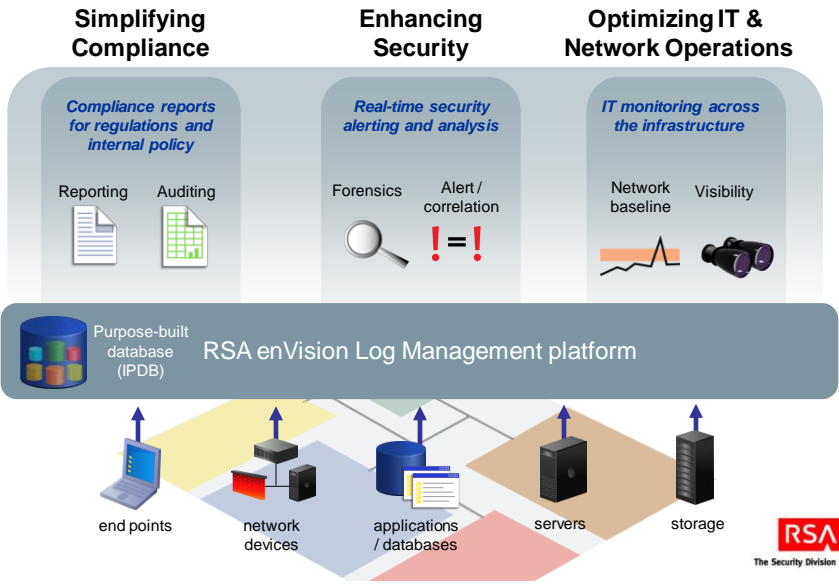




# RSA enVision 3-in-1 SIEM Platform



## SIEM and beyond

- ▶ How SIEM grew from a point project to a global solution ?
  - Log Life Cycle Management & Log Retention
  - Log Assurance
  - SOC & Incident Management



## Log Life Cycle Management

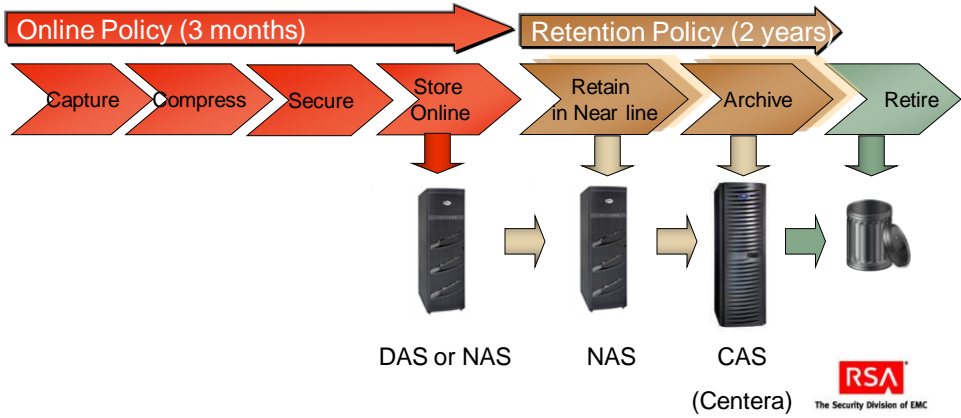
- ▶ **Customer:** Telco
- ▶ **Problem:** Need to comply with EU regulation
  - Must retain logs for year(s)
- ▶ **Solution**
  - Combine RSA enVision with EMC on line archiving system Centera



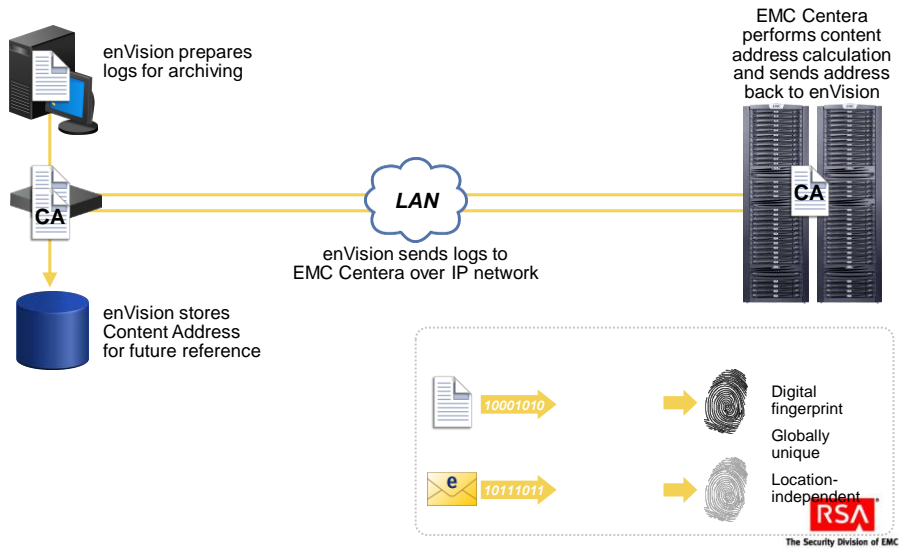
# RSA enVision Secure Storage



- User Defines Log Retention Policies
- RSA enVision automatically helps enforce Storage policies



# How EMC Centera Works: logs archiving



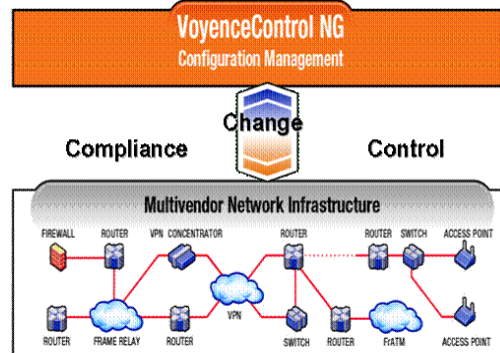
# Log Assurance

- ▶ **Customer:** Large Financial Operator
- ▶ **Problem:** Are devices really sending log events?
  - Security ops can not validate nor control Device Configuration
  - Impact to compliance – ensuring that all infrastructure elements are logging properly and can be audited
- ▶ **Solution**
  - Combine RSA enVision with EMC Voyence
  - Voyence Compliance Engine continually verifies network and enforces RSA enVision as destination log server



# VoyenceControl

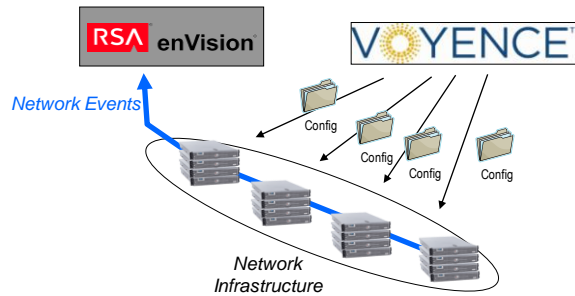
- ▶ Automated Network Compliance, Change and Configuration Management
- ▶ Network Discovery and Configuration Repository
- ▶ Enforce Standards-Based Network Change Processes
- ▶ Enforce Standards and Policies for Network Compliance
- ▶ Automated Network Change Execution



## Log Assurance: Solution

• **Benefits:**

- Increases accuracy of SIEM (enVision) compliance reports
- Decreases risk by logging from entire network



The Security Division of EMC