Building Highly Available Log Management and SIEM Solutions

Sesh Ramasharma, CISSP
Principal – Identity, Access & Security Management
Novell, Inc

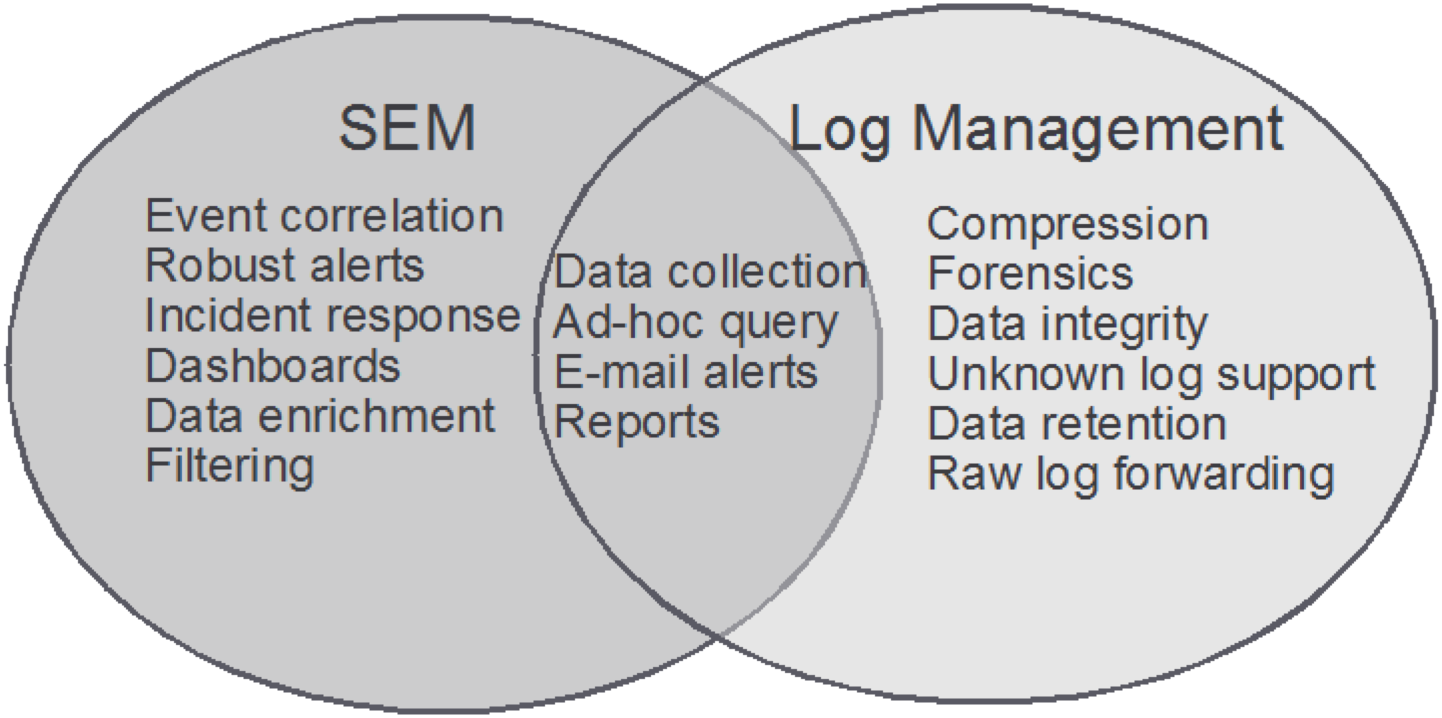
March 2010

Agenda

- Logical view of Log Management and SIEM
- Key Tenants of Security - CIA
- Availability Defined
- Know the moving parts of the solution
- Key considerations
- Tools in the Repertoire
- Summary

Log Management and SIEM*

- Log Management is sometimes referred to as Security Information Management or “SIM”
- Security Event Management or “SEM” is focused on real-time monitoring, alerting, incident response



SEM

Event correlation
Robust alerts
Incident response
Dashboards
Data enrichment
Filtering

Data collection
Ad-hoc query
E-mail alerts
Reports

Log Management

Compression
Forensics
Data integrity
Unknown log support
Data retention
Raw log forwarding

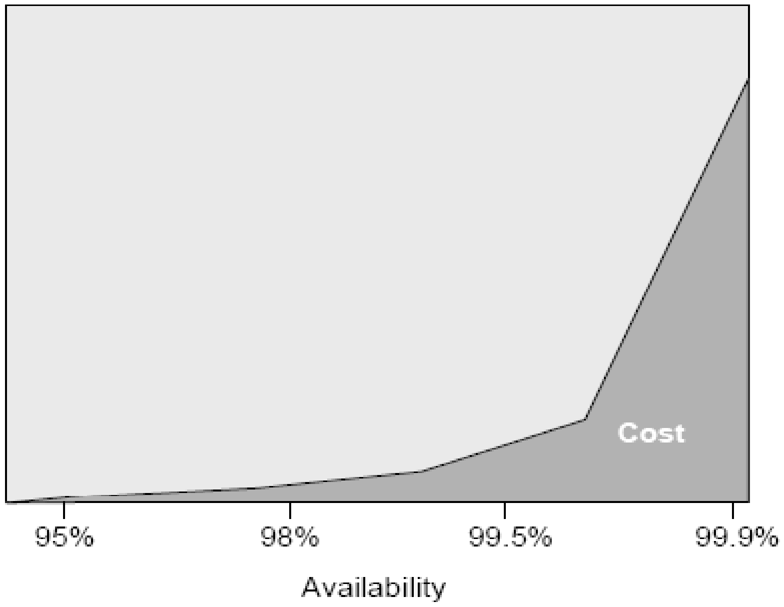
CIA Tenants of Security

- CIA tenants of security apply to SIEM / Log Management systems as well
  - **Confidentiality:** Classification of data and ensuring data is visible to only constituencies that are authorized
  - **Integrity:** Data cannot be tampered with and non-repudiation
  - **Availability:** Available when and where needed

Risk based definition of High Availability

- Definition of “High Availability” is subjective
  - Defined by number of 9’s
- It should be driven by and be commensurate to business risk
- Primary reason it needs to be evaluated subjectively is because it comes with a cost!

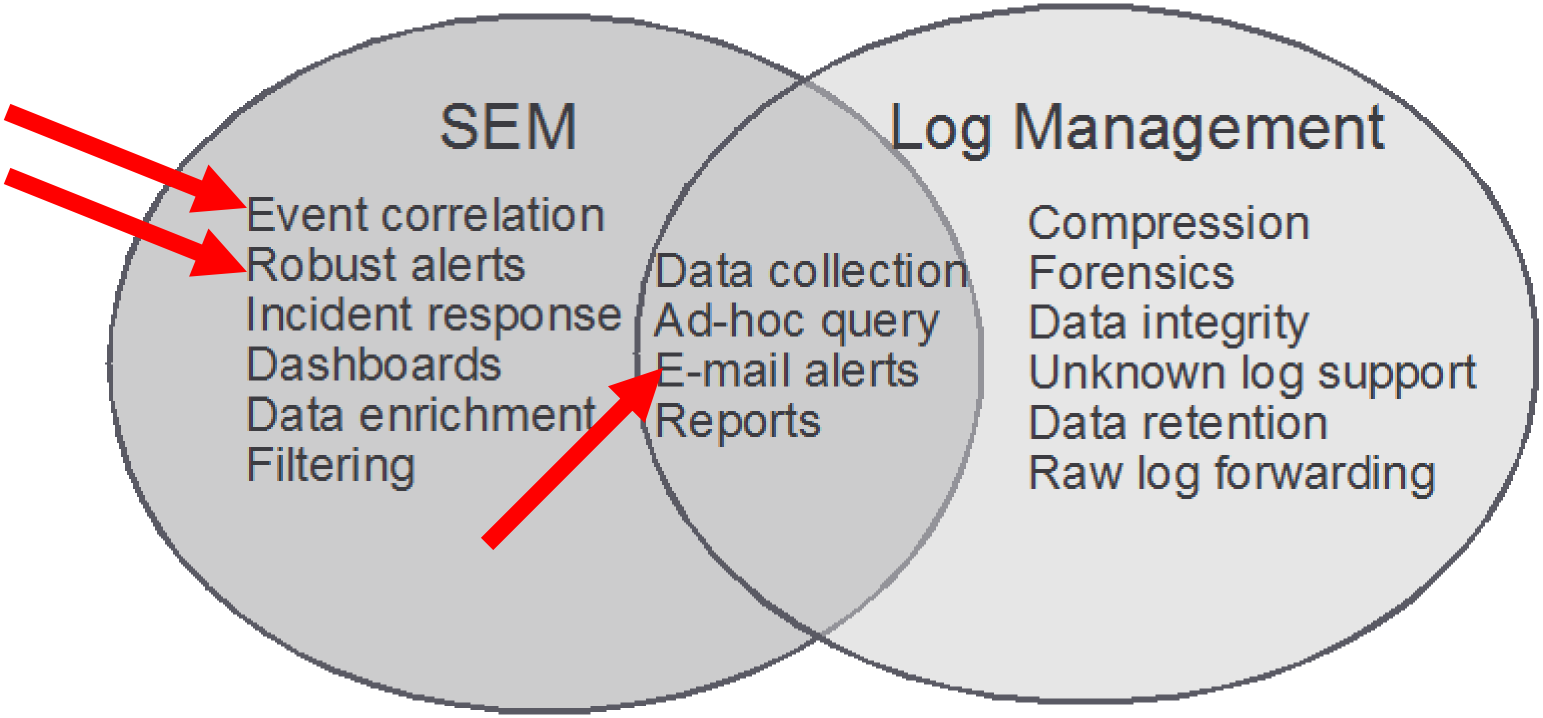
Availability Cost Curve



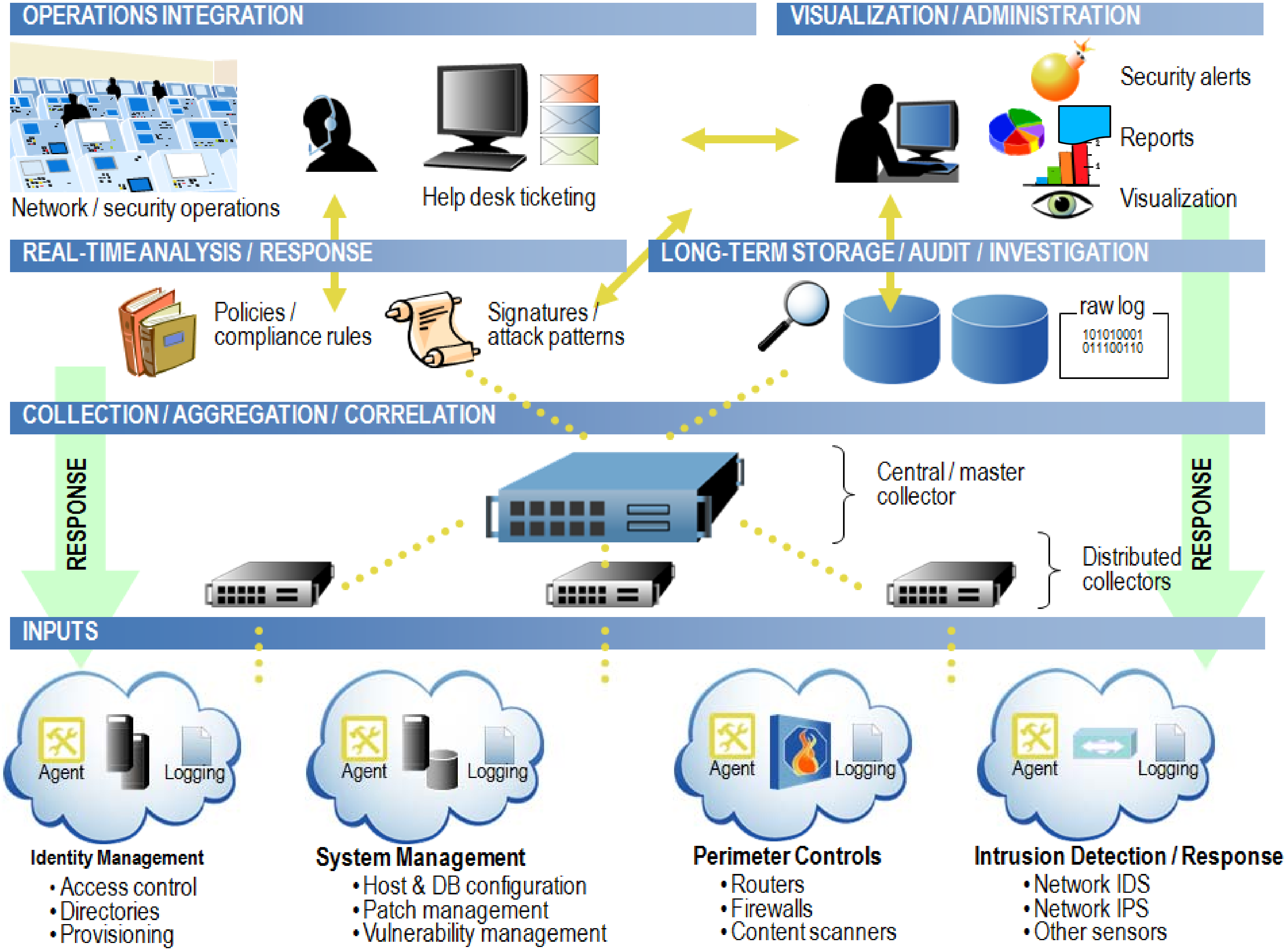
Source: Gartner Research

Functional Sensitivity to Availability

- Break down availability by functionality
- Some functions need higher availability than others

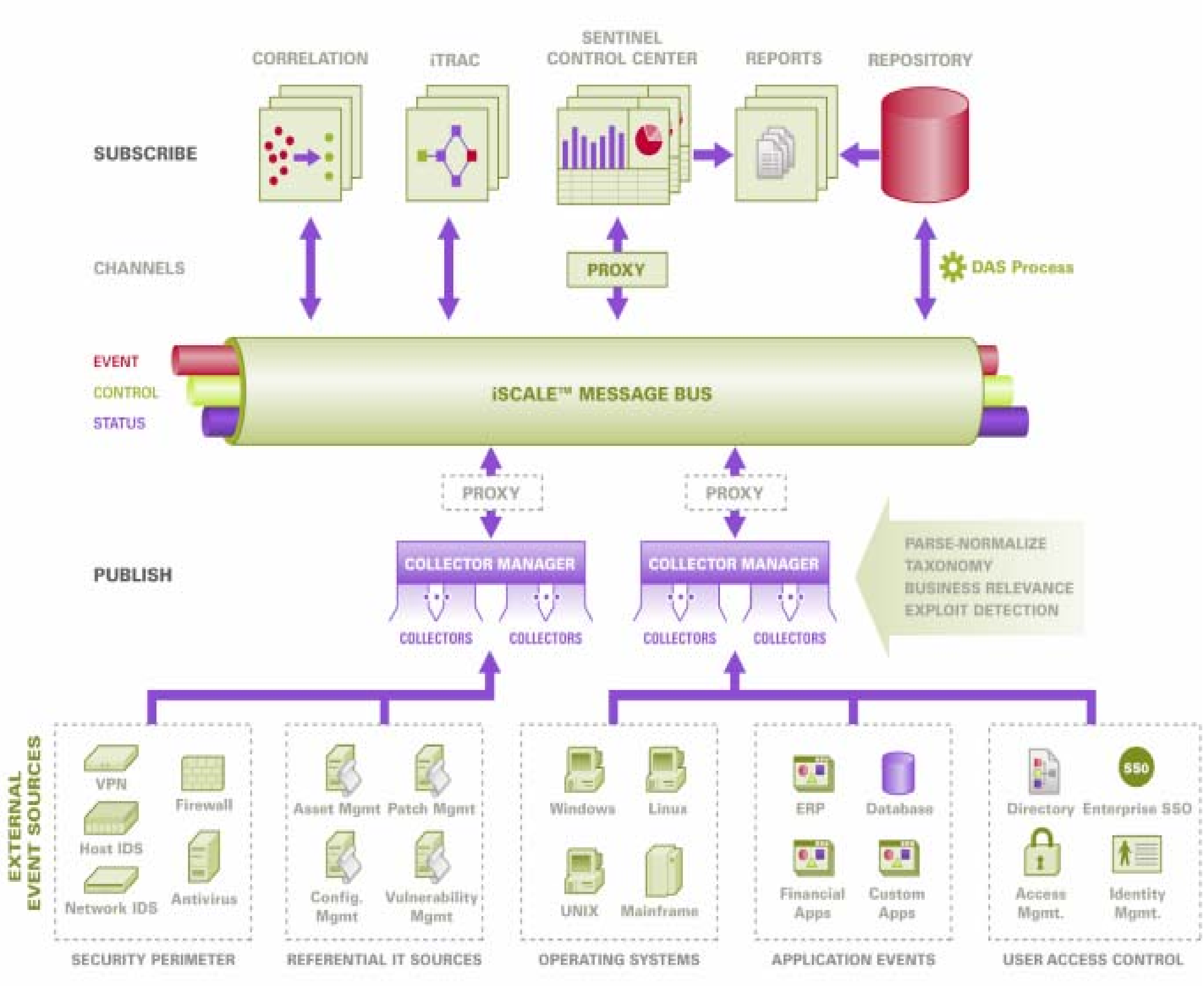


Logical View – SIEM Burton Reference Model

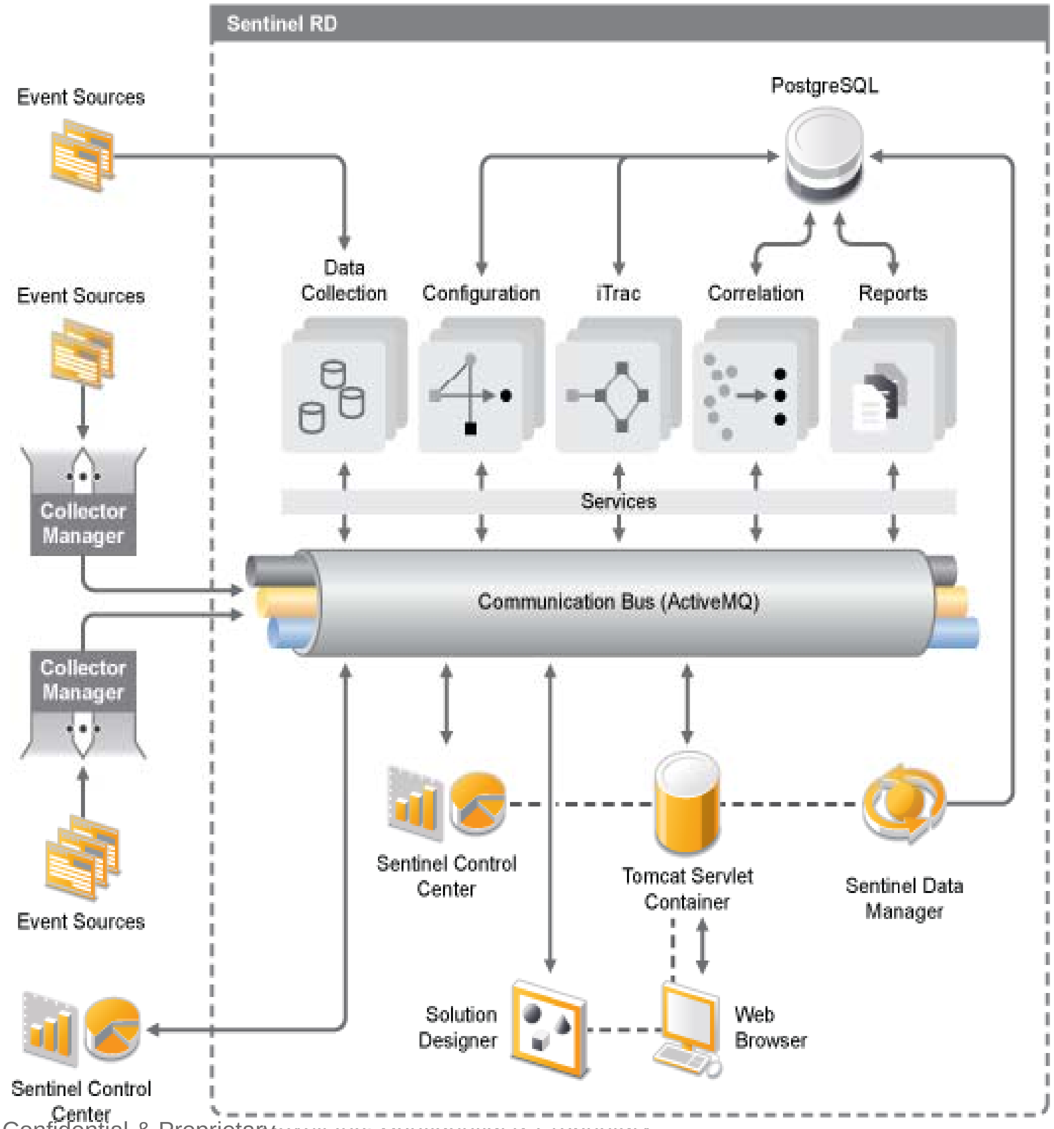


Source: Burton Group –Diana Kelley

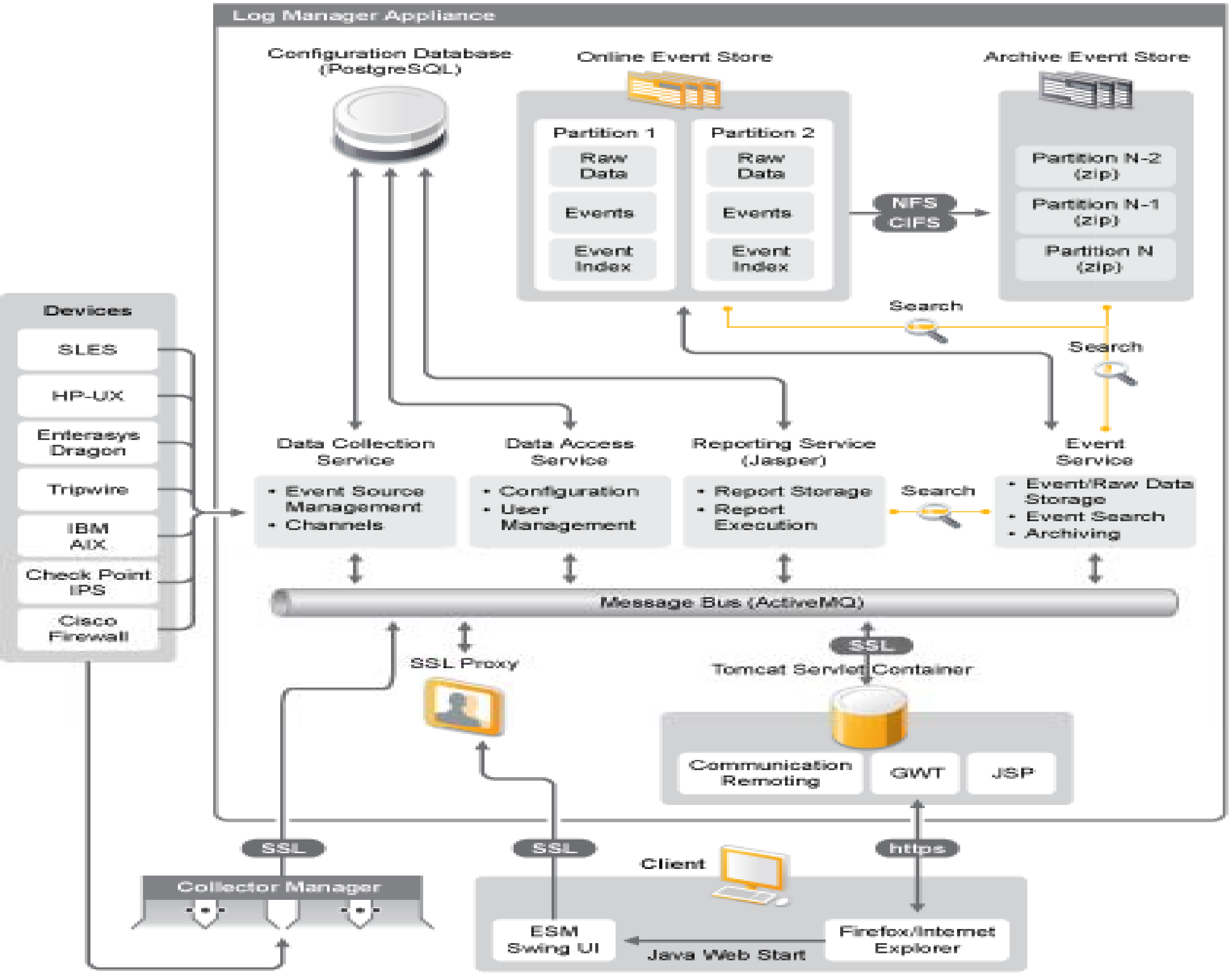
Sentinel SIEM*



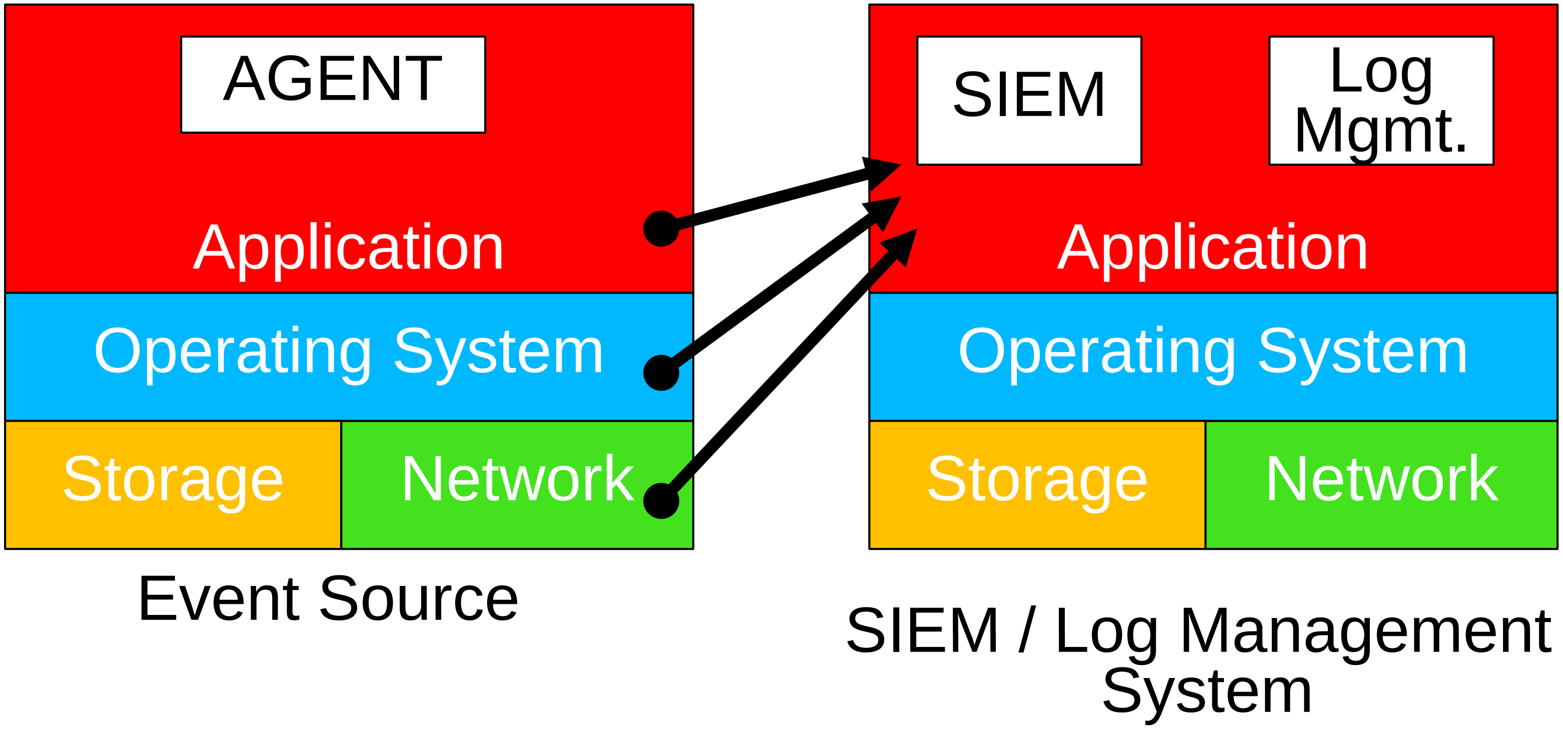
Sentinel RD*


Sentinel RD
Event Sources
PostgreSQL
Event Sources
Data Collection
Configuration
iTrac
Correlation
Reports
Collector Manager
Services
Communication Bus (ActiveMQ)
Collector Manager
Sentinel Control Center
Tomcat Servlet Container
Sentinel Data Manager
Event Sources
Solution Designer
Web Browser
Sentinel Control Center

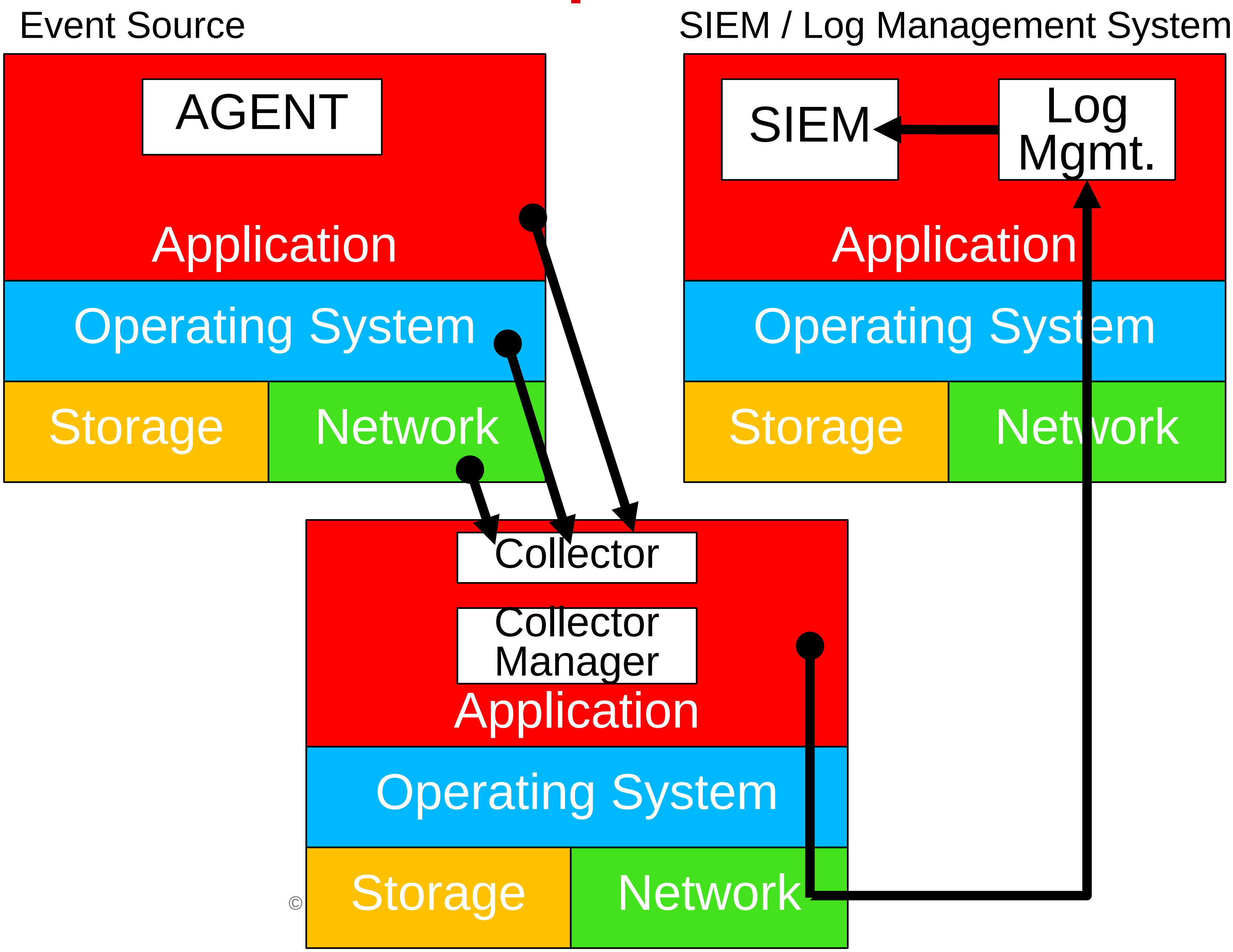
Sentinel Log Manager*



SIEM/Log Management Layers

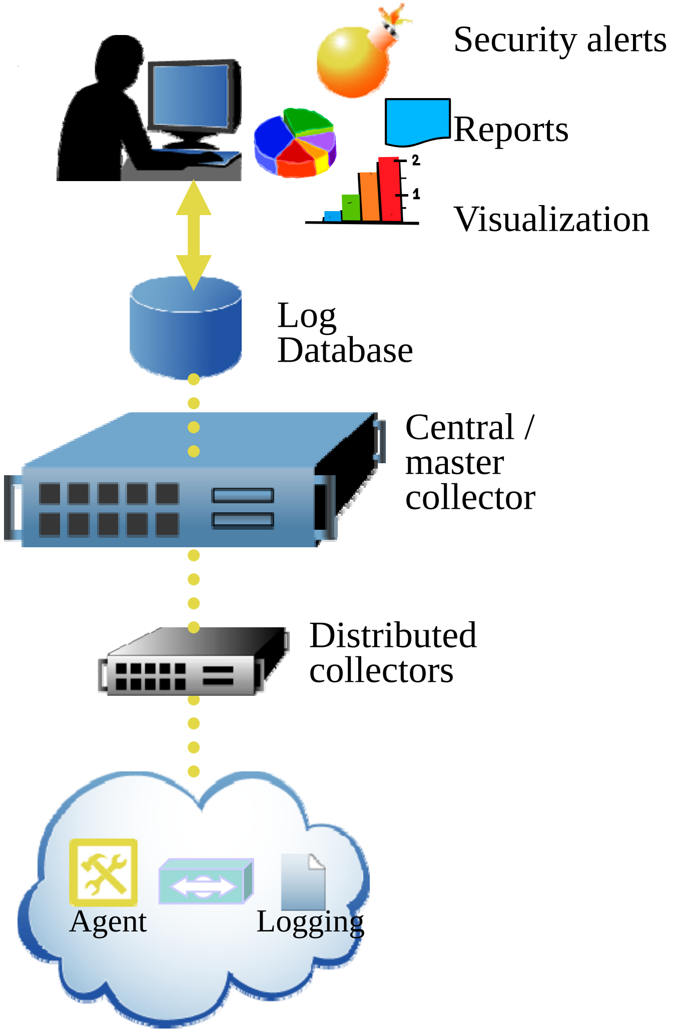


SIEM/Log Management Layers – Sentinel Suite Perspective



Know the Moving Parts - A Vertical Slice – Flavor 1

Burton Reference



Security alerts

Reports

Visualization

Log Database

Central / master collector

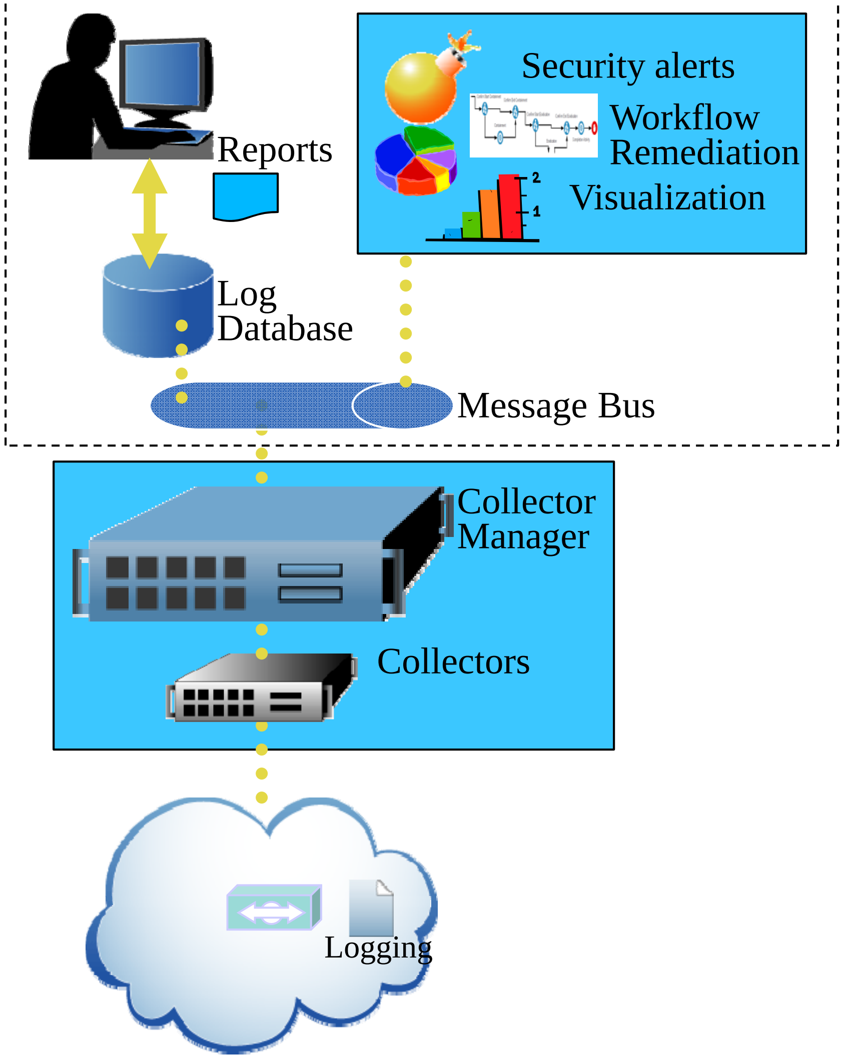
Distributed collectors

Agent

Logging

Event Source

Novell Sentinel



Reports

Security alerts

Workflow Remediation

Visualization

Log Database

Message Bus

Collector Manager

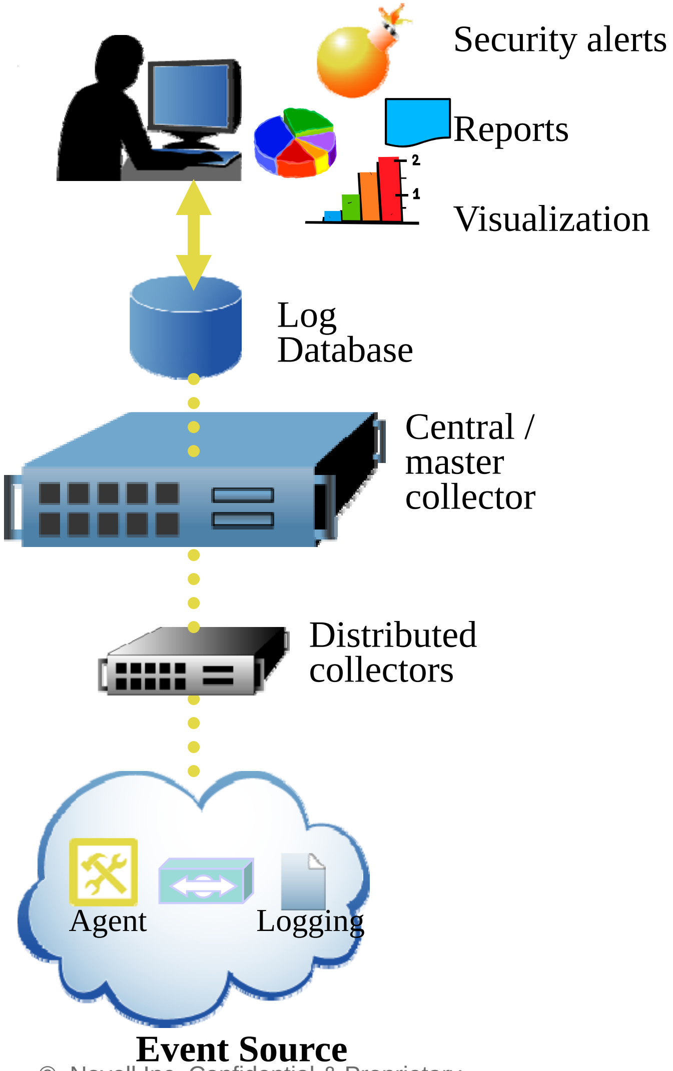
Collectors

Logging

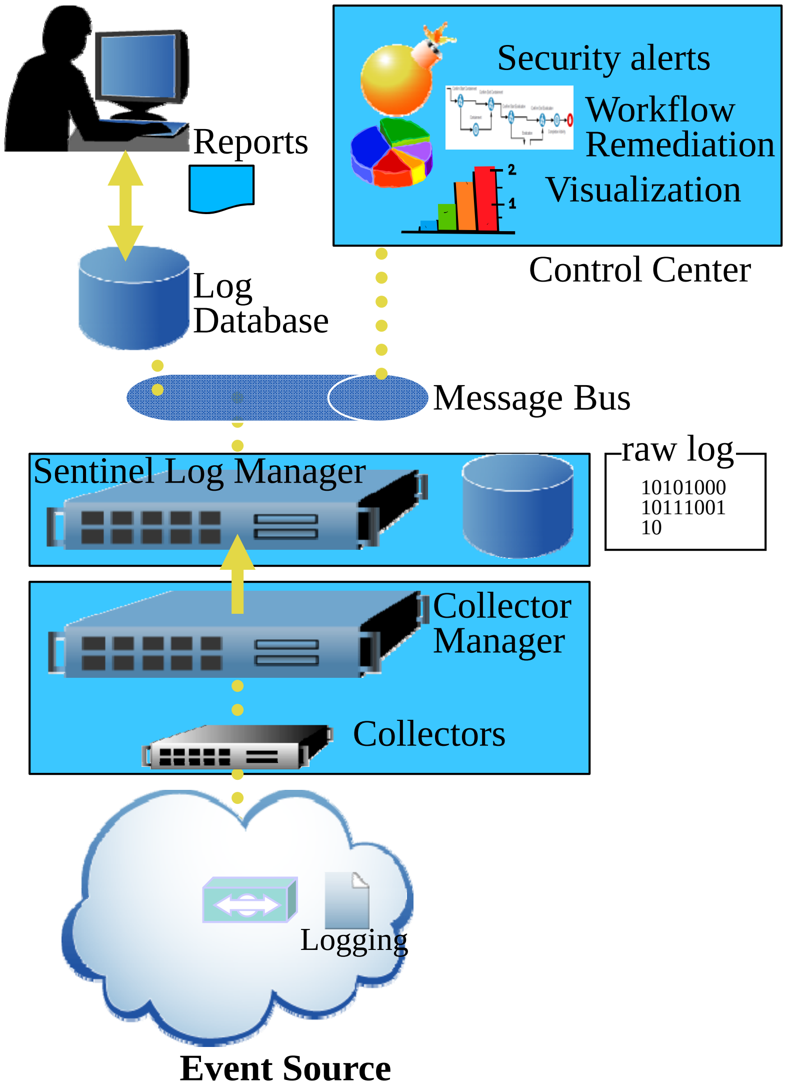
Event Source

Know the Moving Parts - A Vertical Slice – Flavor 2

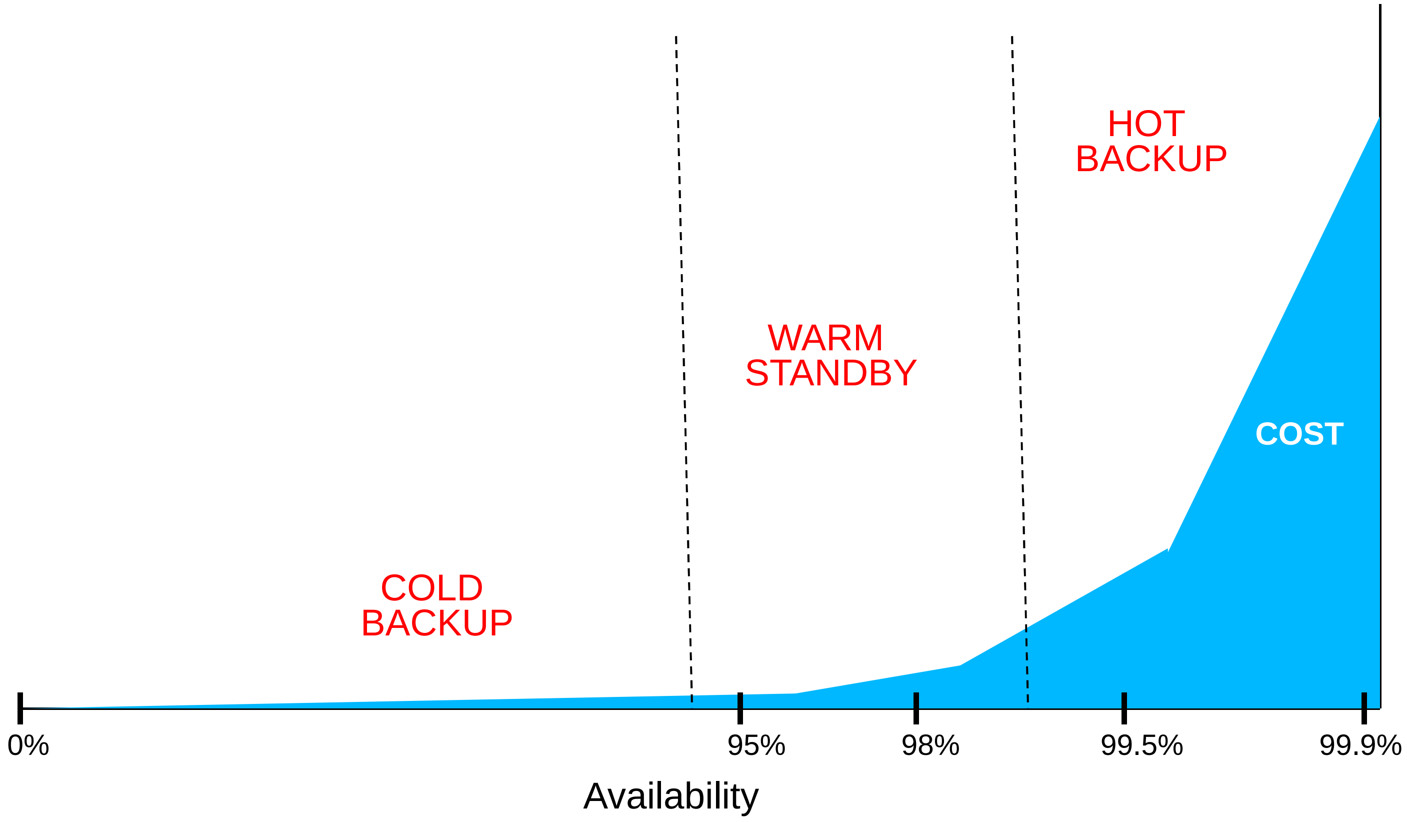
Burton Reference



Novell Sentinel



Degrees of Availability



Cold Backup

Characteristics

- Backup all the components at periodic intervals
- Restore a point-in-time backup upon failure

Implications

- Economic solution
- Availability will be on the lower spectrum as recovery will take longer time
- State of the entire system has to be in synch
- High potential for data loss upon recovery

Warm Standby

Characteristics

- Backup all the components at periodic intervals
- Full redundant system on stand-by
- Restore a point-in-time on a redundant hardware on stand-by mode
- Activate stand-by upon primary failure

Implications

- More expensive than cold backup solution
- Availability will be better
- State of the entire system has to be in synch
- Potential for data loss on recovery

Hot Backup

Characteristics

- Full redundant system
- Collect events redundantly from all event sources
- Activate stand-by upon primary failure
- Can be used in an Active/Active mode if correlation rules and reporting users are high

Implications

- More expensive than cold backup and warm standby solution
- Availability will be best
- Low potential for data loss on recovery

Hybrid Solutions are possible

- It is possible to have hybrid solutions to achieve varying degree of availability for different components / event sources based on business requirements and cost factors.
  - High Availability within a Data Center
    - E.g - Clustering solution with RAID
      - Protects against outage of hardware or components within a data center
  - High Availability Across Data Center
    - E.g - Warm standby across data center
      - Protects against outage of entire data center
  - Disaster Recovery
    - E.g - Cold backup every day
      - Protects from total loss of service in case of failure / disaster

Question for the audience –
What else is possible to provide each of these situations?

Key Considerations for model choice

- Functional Sensitivity
- Distributability of the solution
  - More is better or less is better? – Depends!!!
- Balance Scalability with Availability
- Appliance vs Software
  - Component Distributability
  - Component Resiliency
    - Redundancy
    - Local Buffering
- Self-monitoring capabilities
  - Need a MoM or can your SIEM software monitor itself

Tools in the Repertoire

- Traditional
  - Vendor provided solution
    - Full redundancy?
  - Platform HA
    - E.g OHAC, HACMP
  - O/S HA
    - E.g Veritas clusters, Linux Clusters, Solaris clusters
  - Database HA
    - Oracle clustering, MS-SQL clustering
  - Disk HA
    - E.g SANs, EMC, RAID
  - Network HA
    - E.g Self healing networks
- Leading Edge / Emerging
  - Cloud Computing
  - Intelligent Workload Management

Summary – Back to Basics

Consider a Systemic View

+Understand the organizational risks and costs of these risks materializing

+Know the cost / benefit of SIEM HA for your organization

+Attack HA from a functional point of view

+Understand the moving parts

+Leverage tools available at all layers

Build the best HA solution for your organization

Novell®