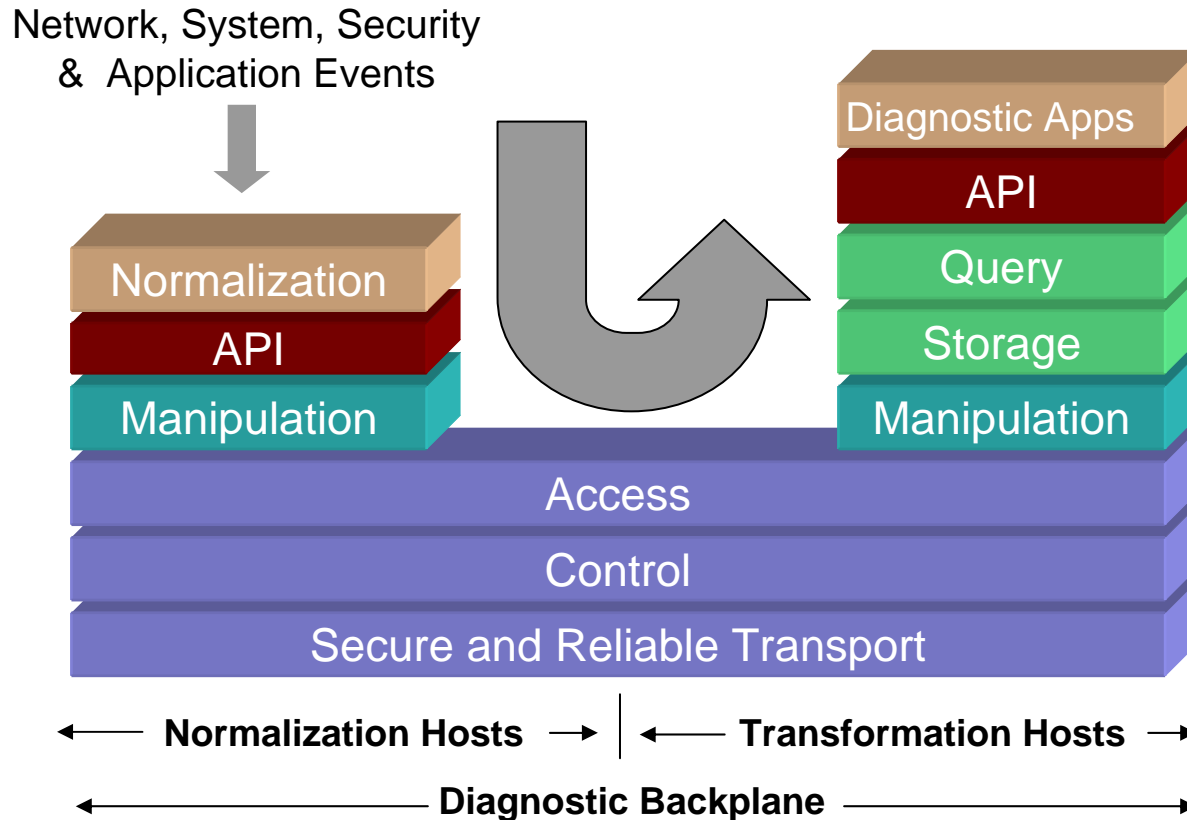




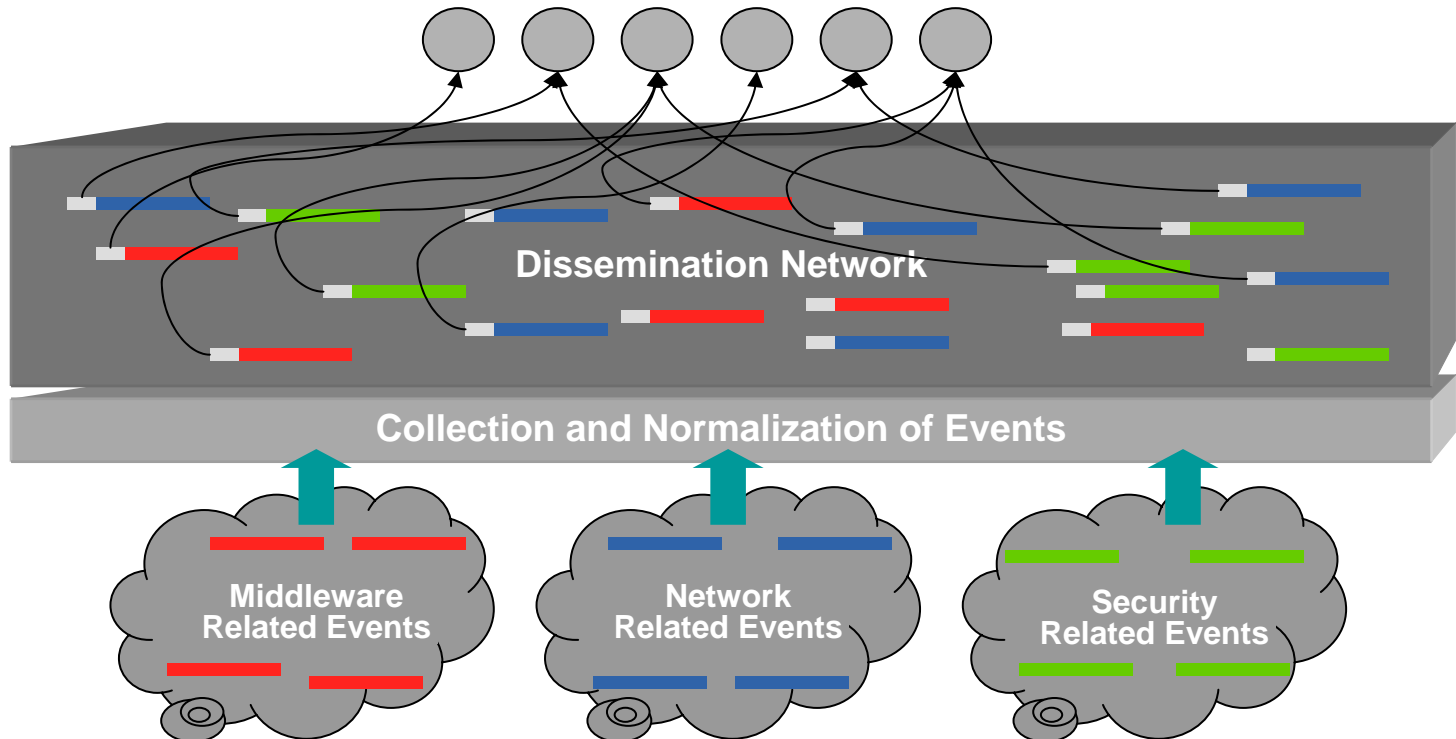
# Diagnostic Backplane

# Core middleware diagnostic model



# Enabling Diagnostic Applications With a Common Event Descriptor

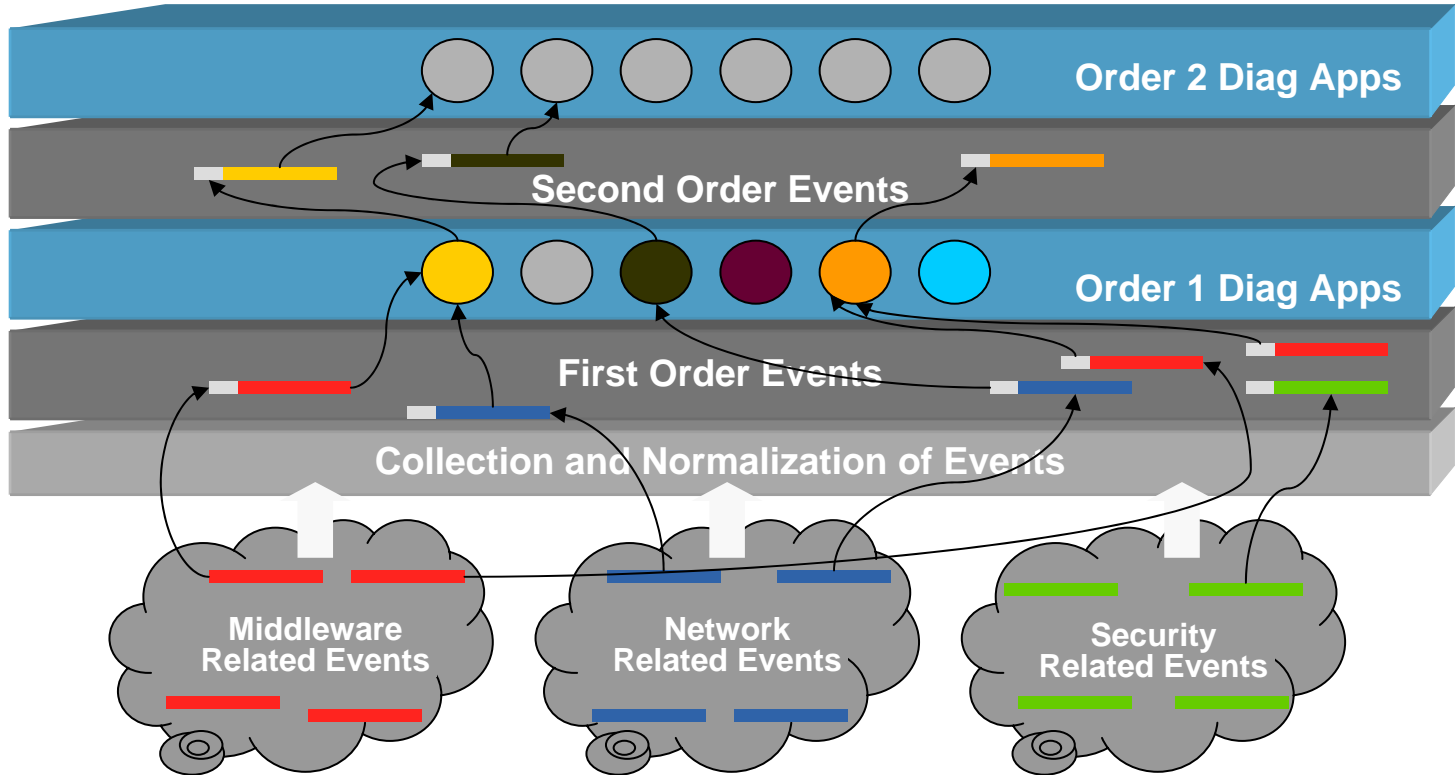
Diagnostic applications (Middleware, Network, Security) can extract event data from multiple data sets



# Multiple Levels of Diag Apps Producing High Order Event Records

- First Order Events:
  - Passive: /var/log/\*, NetFlow, SNMP traps
  - Active: OWAMP measurement, iperf, notification of a measurement system
- Second Order Events
  - Combines multiple types of events to give a higher level of information
  - Example: using NetFlow, /var/log/httpd-\* and /var/log/messages to generate the event “DOS attack on web server web23.foo.edu.

# Multiple Levels of Diag Apps Producing High Order Event Records



# Architecture

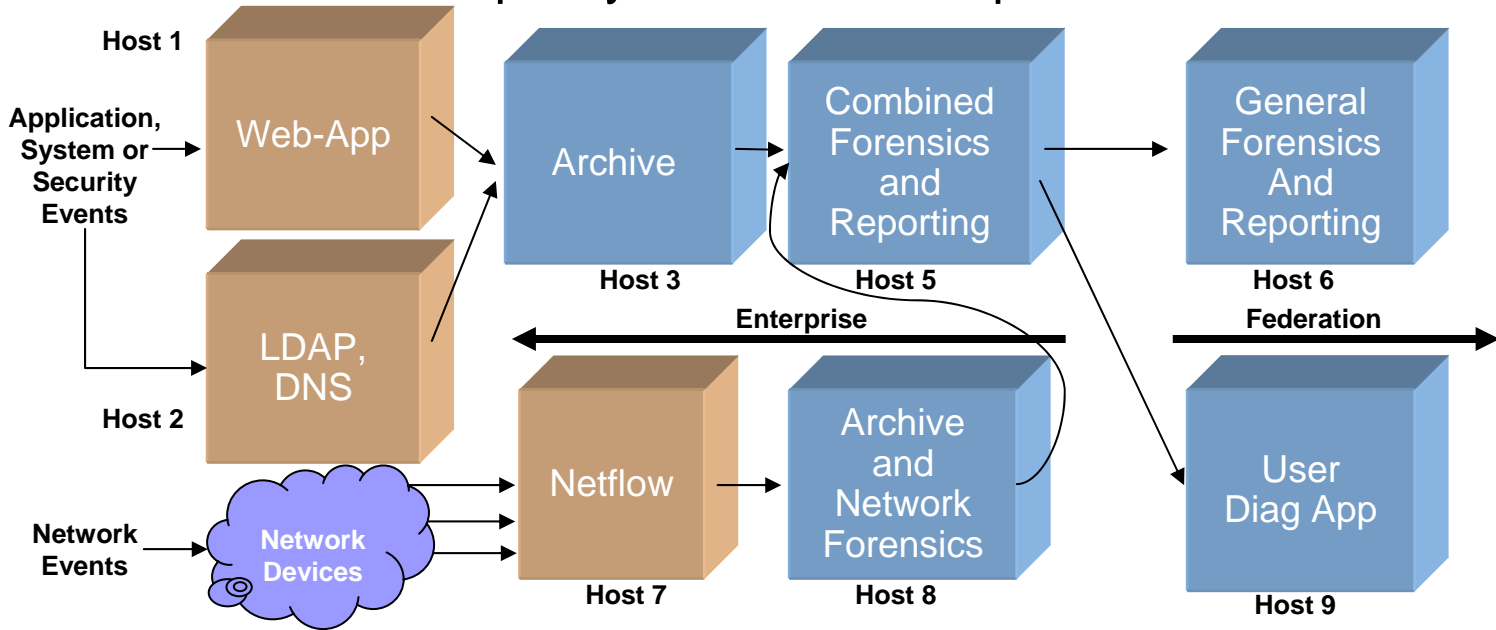
- **Normalization agents:** convert raw events into common event records (CER)
- **Forwarding agents:** move CER between storage agents.
- **Storage Agents:** archive CER to files or populate database
- **Transformation agents:** anonymize, aggregate, tag, and prune CERs
- **Application agents:** analyze event data
- **Management agents:** control the diagnostic infrastructure itself.
  - Diagnosis of backplane components
  - Web, GUI and CLI applications for controlling and configuring the overall network of backplane hosts

# Initial Input Sources

- RH9 and Fedora C2 based events
  - Kernel events
  - Syslog
  - /var/log/messages (ssh, cron, named, etc.)
  - /var/log/httpd
- Windows (2000 and 2003 server)
  - User events
  - Security events
  - Application events
  - UInstaller (WMI interface)
- Network events
  - Netflow V5
- Security events
  - Snort

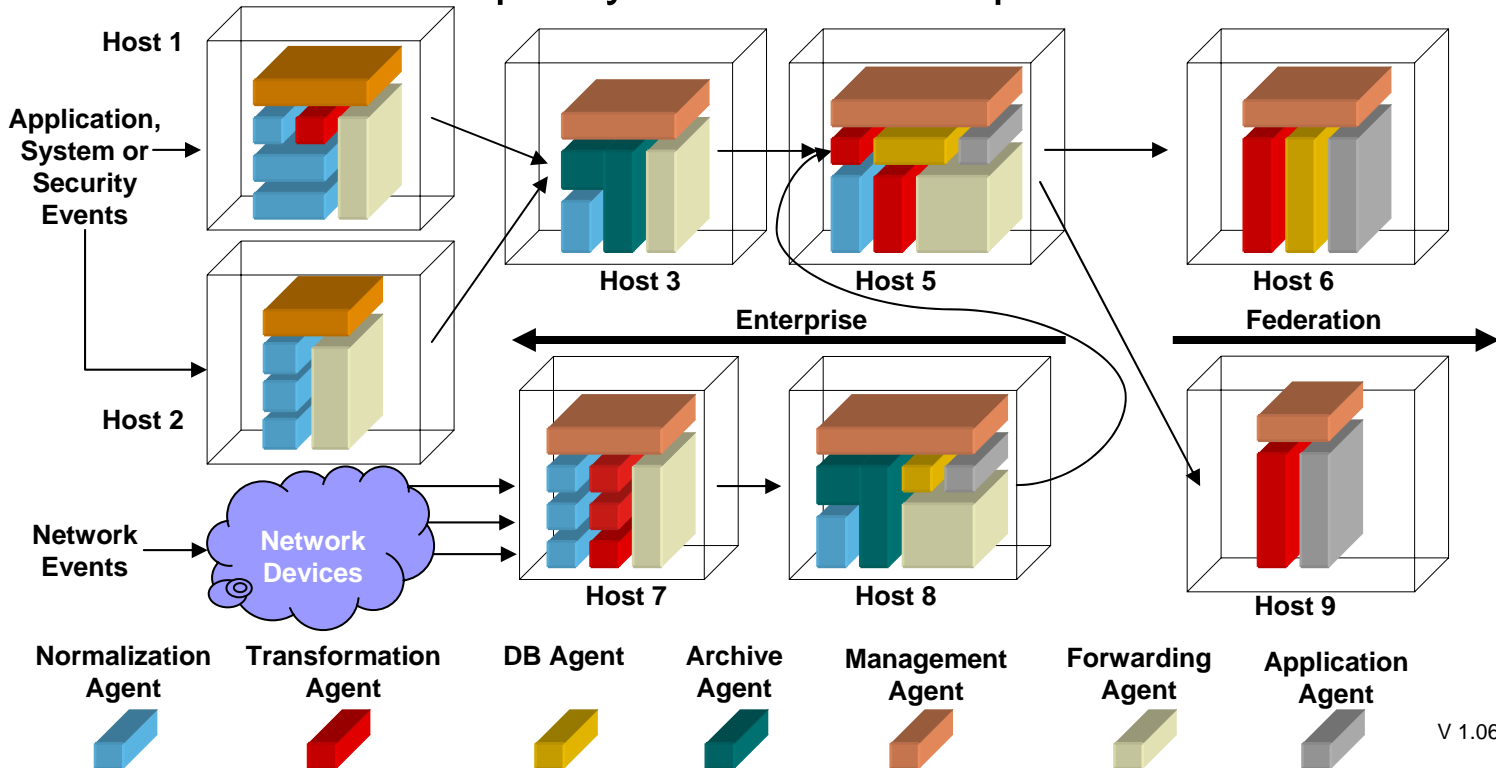
# Event Flows

Event flows can be customized to provide the desired function and policy within an enterprise or federation



# Event Flows

Event flows can be customized to provide the desired function and policy within an enterprise or federation



# Diagnostic Tool Integration

