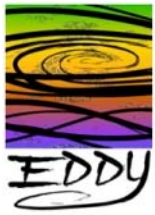


Visual Glossary of EDDY Agents and Their Functions

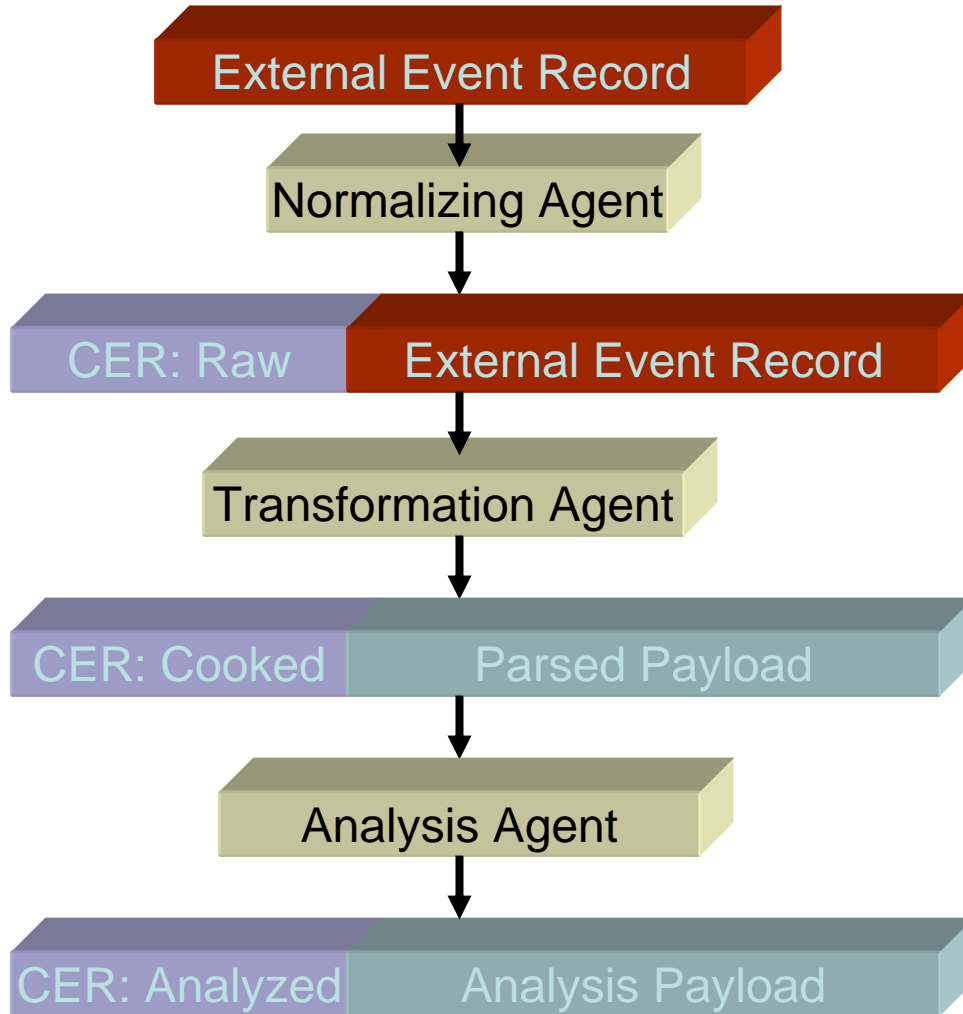
Intended to augment agent description
appendix in the EDDY Development and
Deployment Guide (DDG)

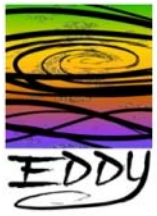
Version 0.54

Copyright Carnegie Mellon 2003-
2008

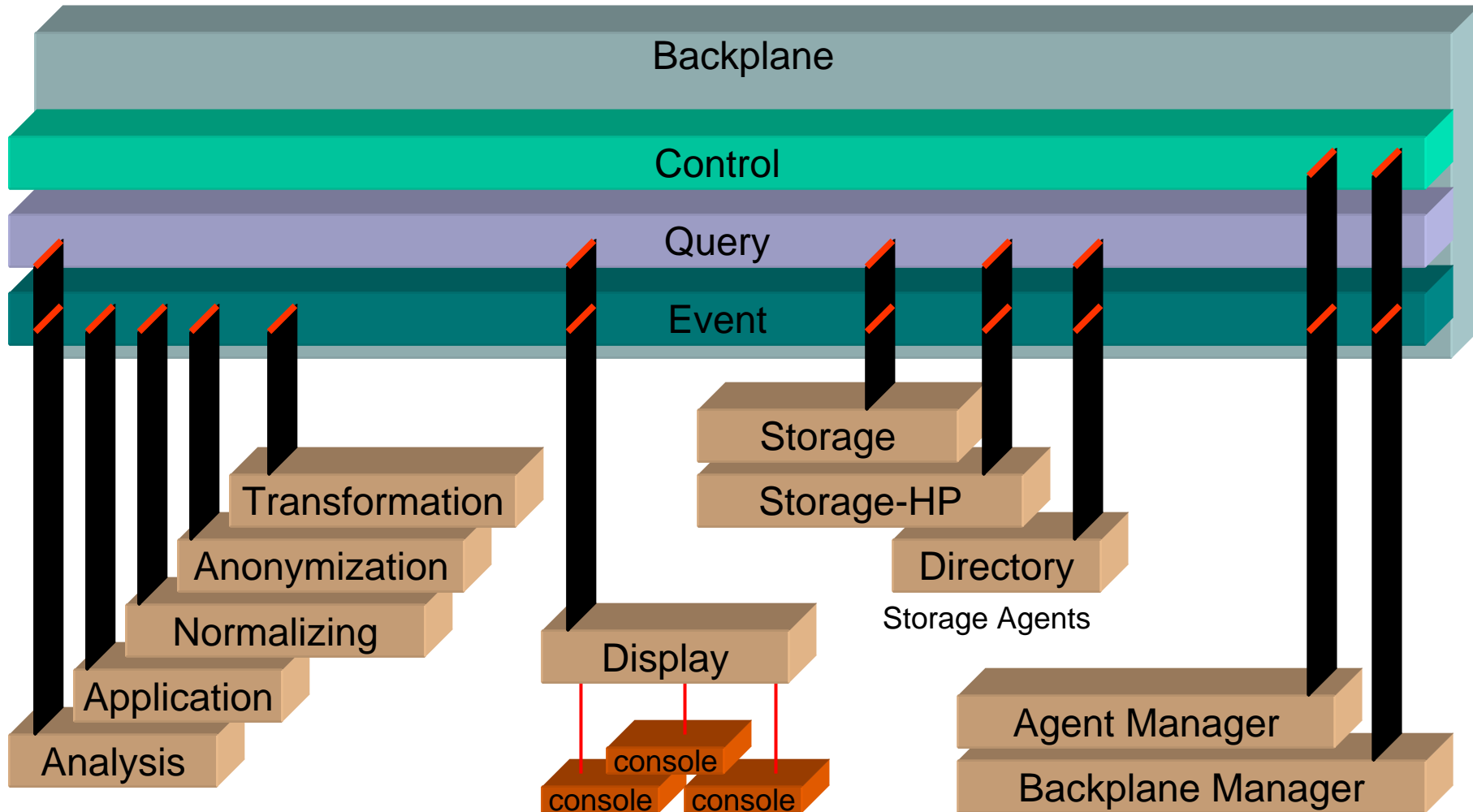


Event Progression





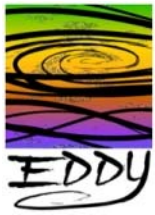
Backplane Transport Channels



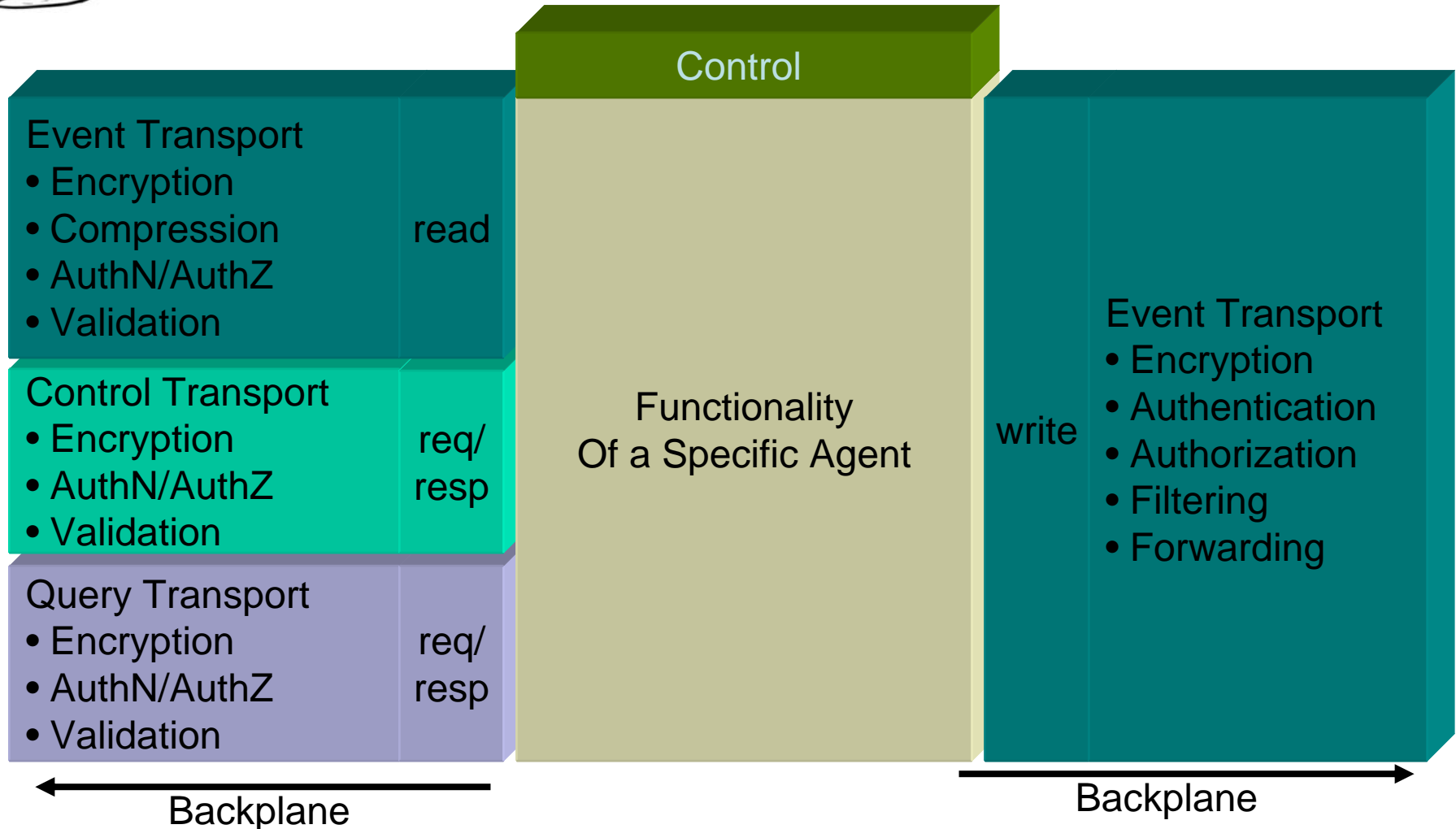
Base Agents

Copyright Carnegie Mellon 2003-
2008

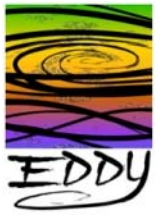
Control Agents



Backplane Channel APIs

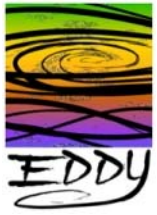


Note: All read and write components can have multiple sources and destinations



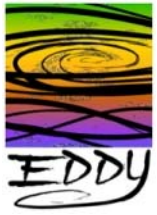
Agent Functionality

- Encryption is optional
- Retry on writes to event channel
- Forwarding (routing) and filtering part of each agent
- Initially, filtering is on output only
- Initially, any on-the-fly changes to an agent must be done by reconfig/restart of agent



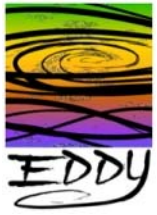
Agent Functionality Notes Cont.

- The following attributes of an agent will be specified in a configuration file
 - event channel interconnects
 - filter rules
 - forwarding rules
 - parameters specific to the agent itself



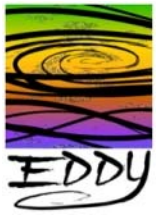
Event Base Agents

- Normalizing
- Transformation
- Application
- Analysis
 - In-Line
 - External
- Display



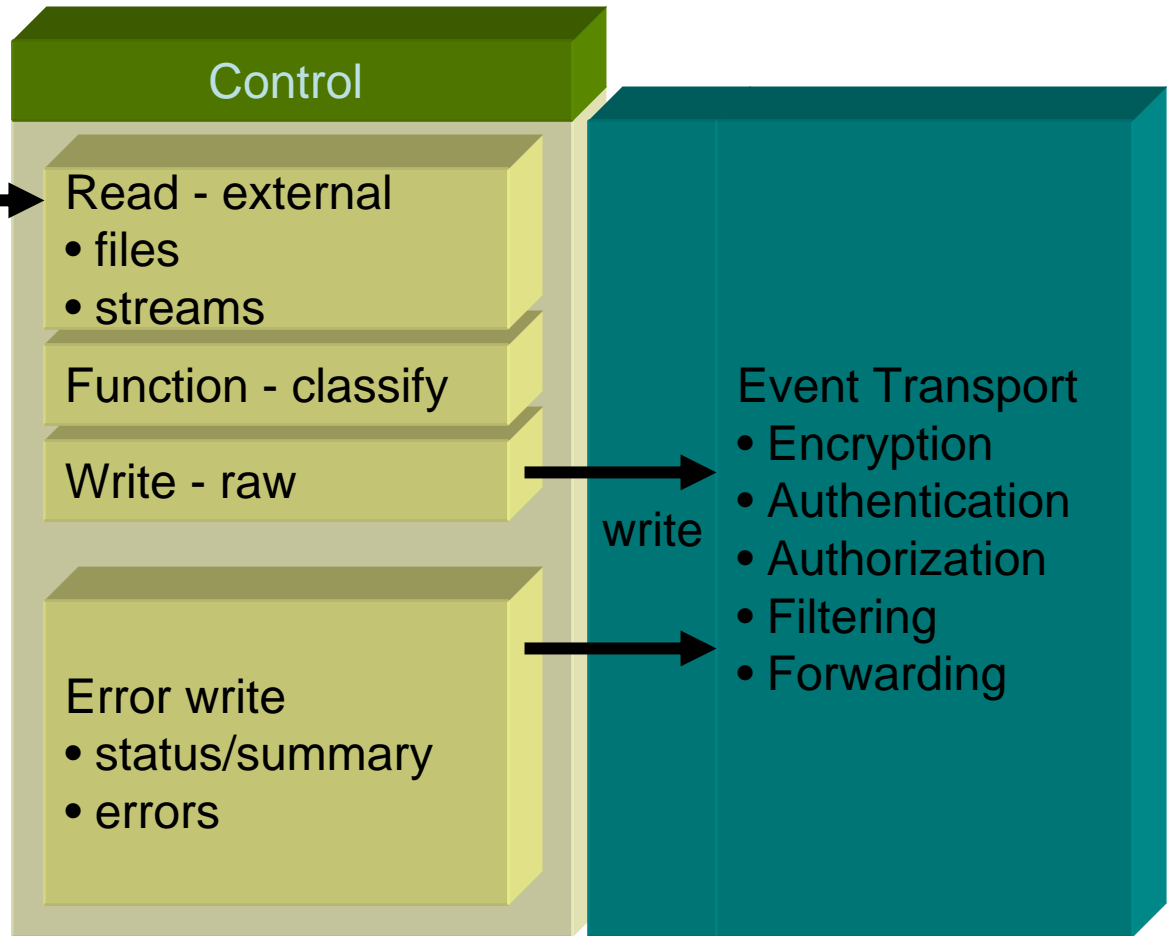
Normalizing Agent (write)

- Function
 - Normalize external events into raw CER events
 - Populate the baseInfo structure of the CER with as much information as possible to aid in correlation
 - External events can be local to a host (/var/log/*) or external (such as Netflow)



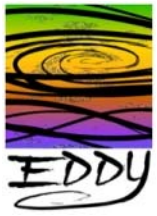
Normalizing Agent (write)

External event data
sources from host and
network devices

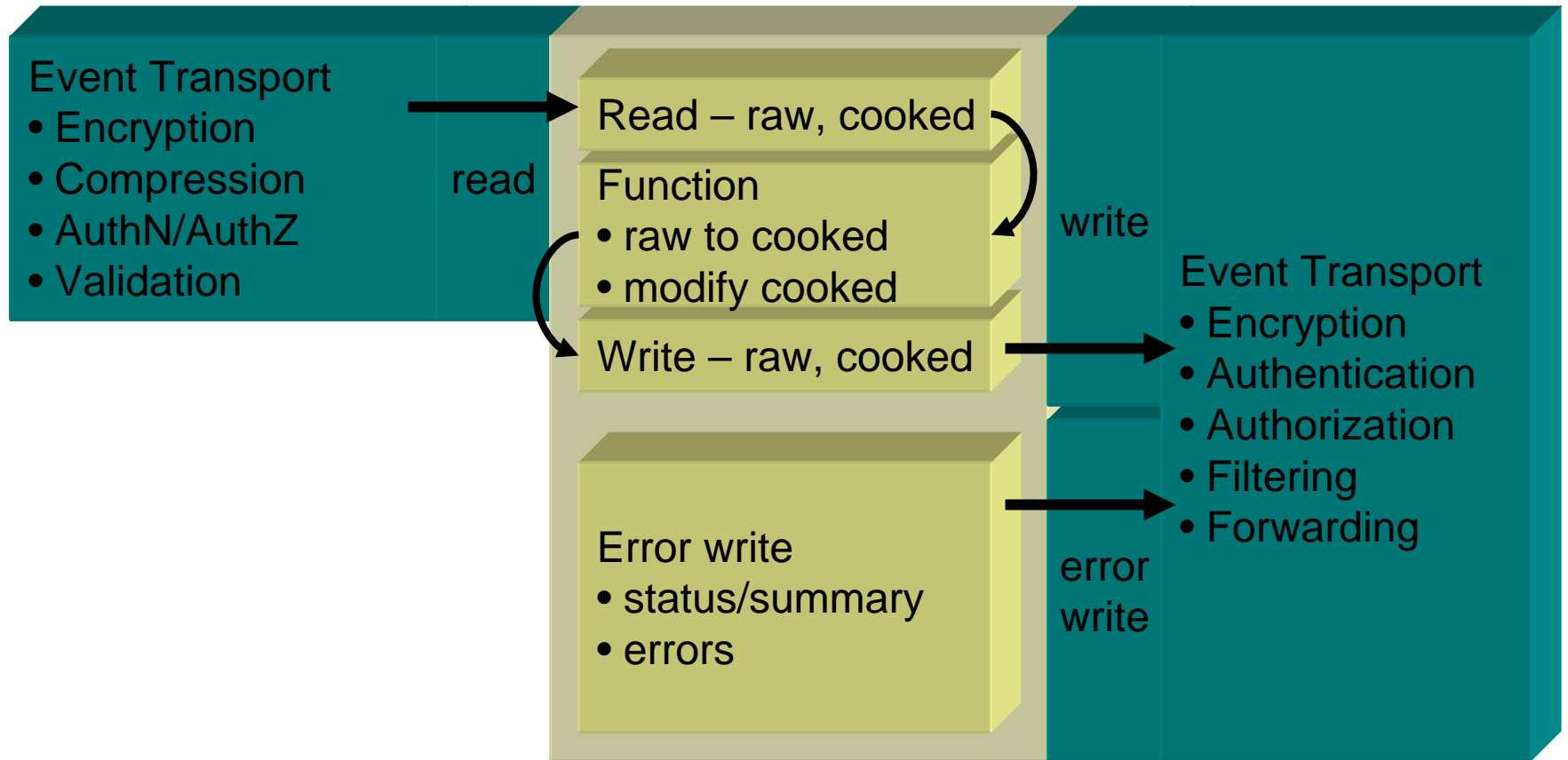


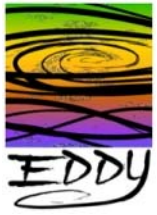
Transformation Agent (read/write)

- Function
 - Transform a raw into cooked CER (XML)
 - Add additional information into the userTag field of the CER
 - Modify one or many fields the CER based on some function such as
 - Static $f(x)$
 - Based on historical observation of past events
 - Query events from the query channel of the backplane and produce some out-of-band action



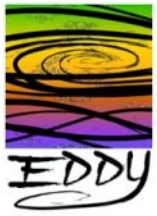
Transformation Agent (read/write)



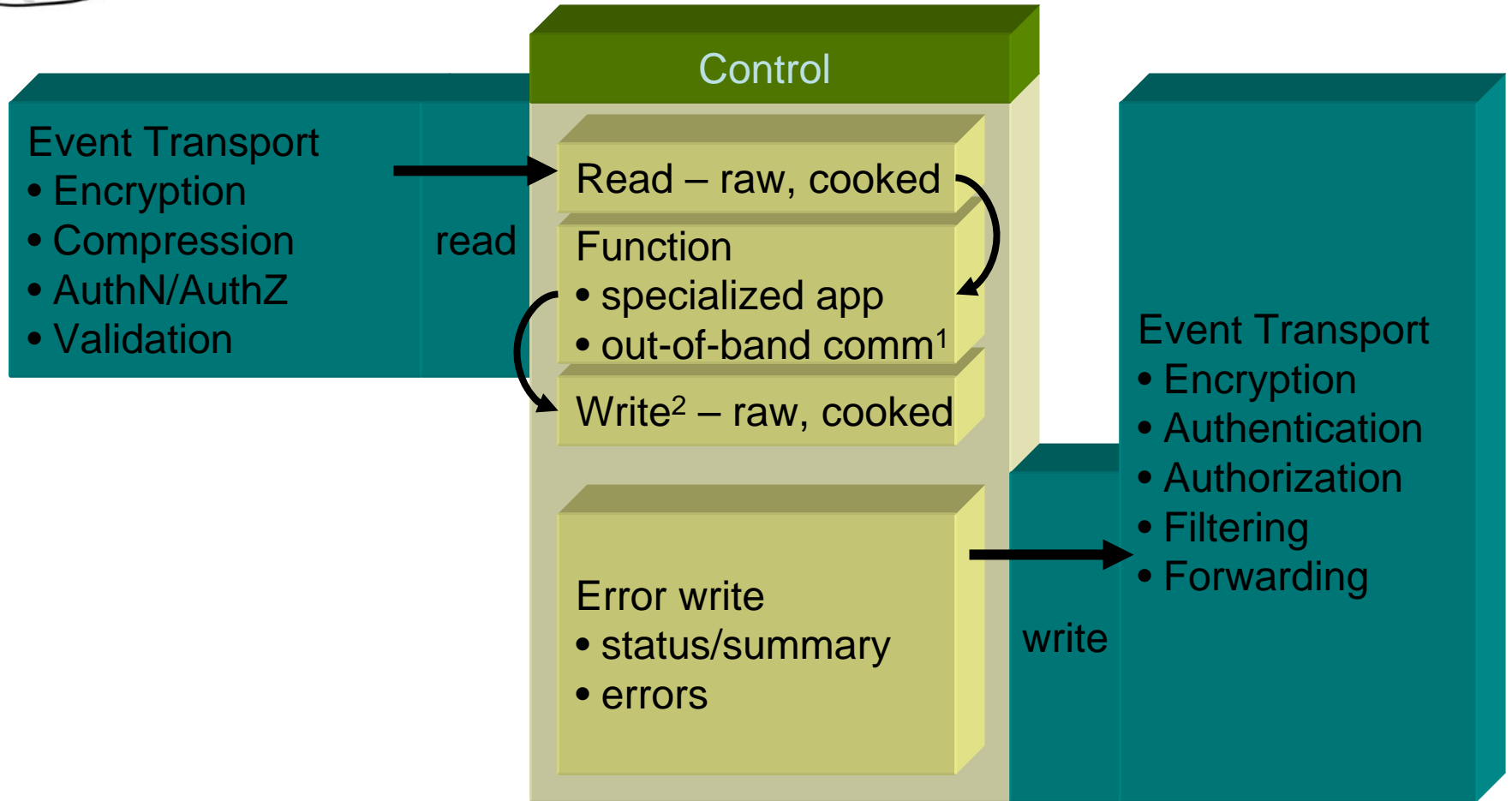


Application Agent (read/write opt.)

- Function
 - Read events from the event channel of the backplane and produce some out-of-band action
 - Query events from the query channel of the backplane and produce some out-of-band action

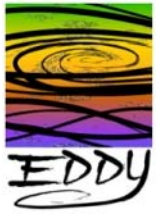


Application Agent (read/write opt.)



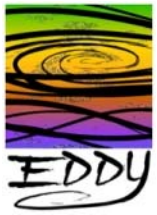
Note 1: An example of out-of-band communication could be to Cricket or SNMP

Note 2: A write to the Event transport channel is optional

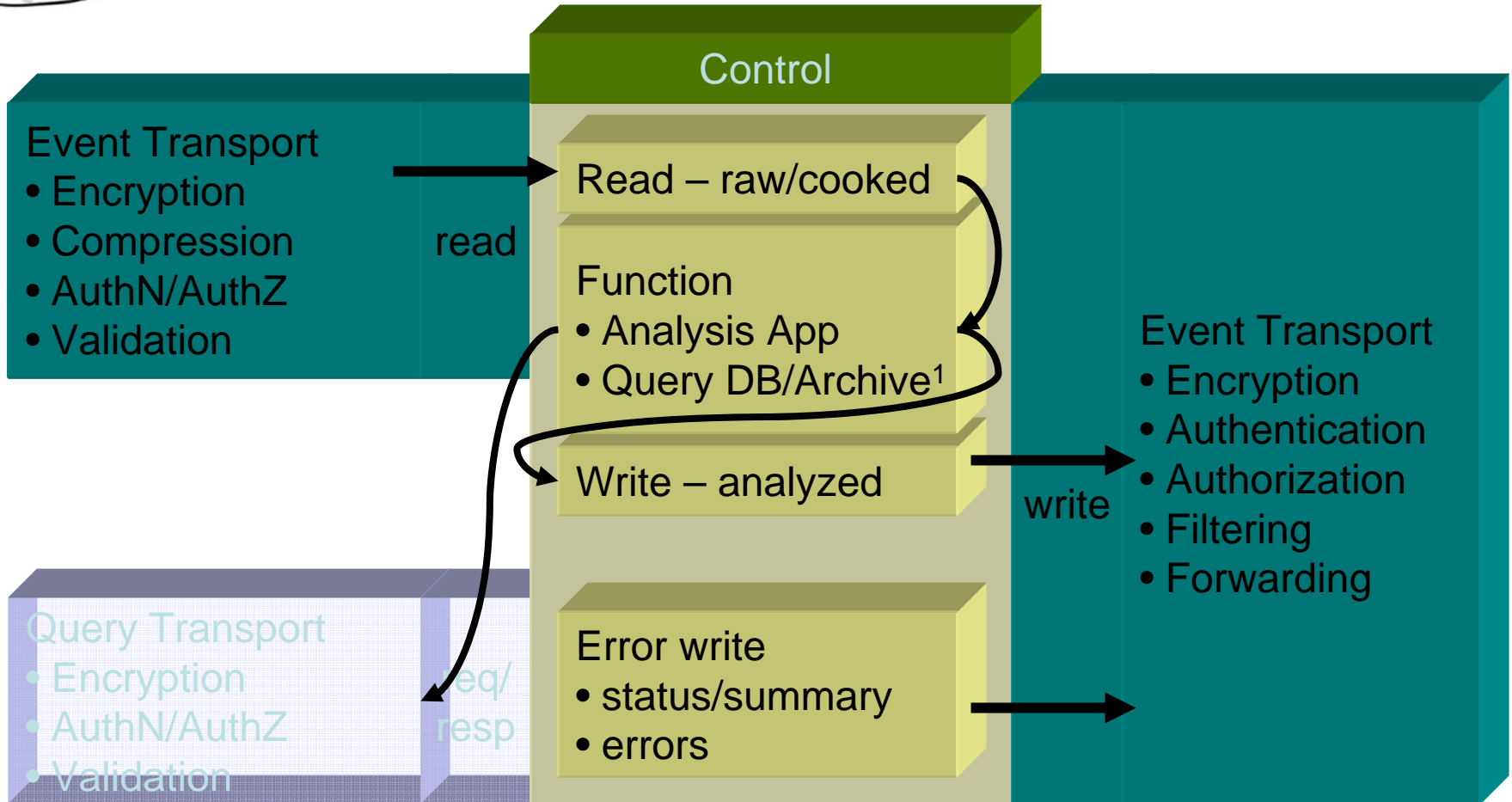


Analysis Agent In-Line (read/write)

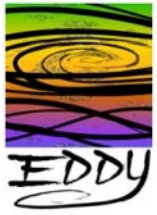
- Function
 - Transform a raw or cooked CERs from the event channel of the backplane to analyzed CER and inject it onto the event channel of the backplane
 - The analyzed CER is based on some function such as
 - Static $f(x)$
 - Based on historical observation of past events



Analysis Agent In-Line (read/write)

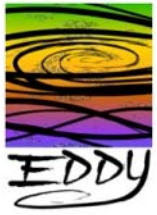


Note 1: A read to the Query channel is optional



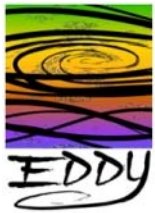
Analysis Agent External (write)

- Function
 - Access the query channel and/or the event channel of the backplane
 - The analysis is based on some function such as
 - Static $f(x)$
 - Based on historical observation of past events
 - Take action on the analysis and use an external method to communicate the analysis

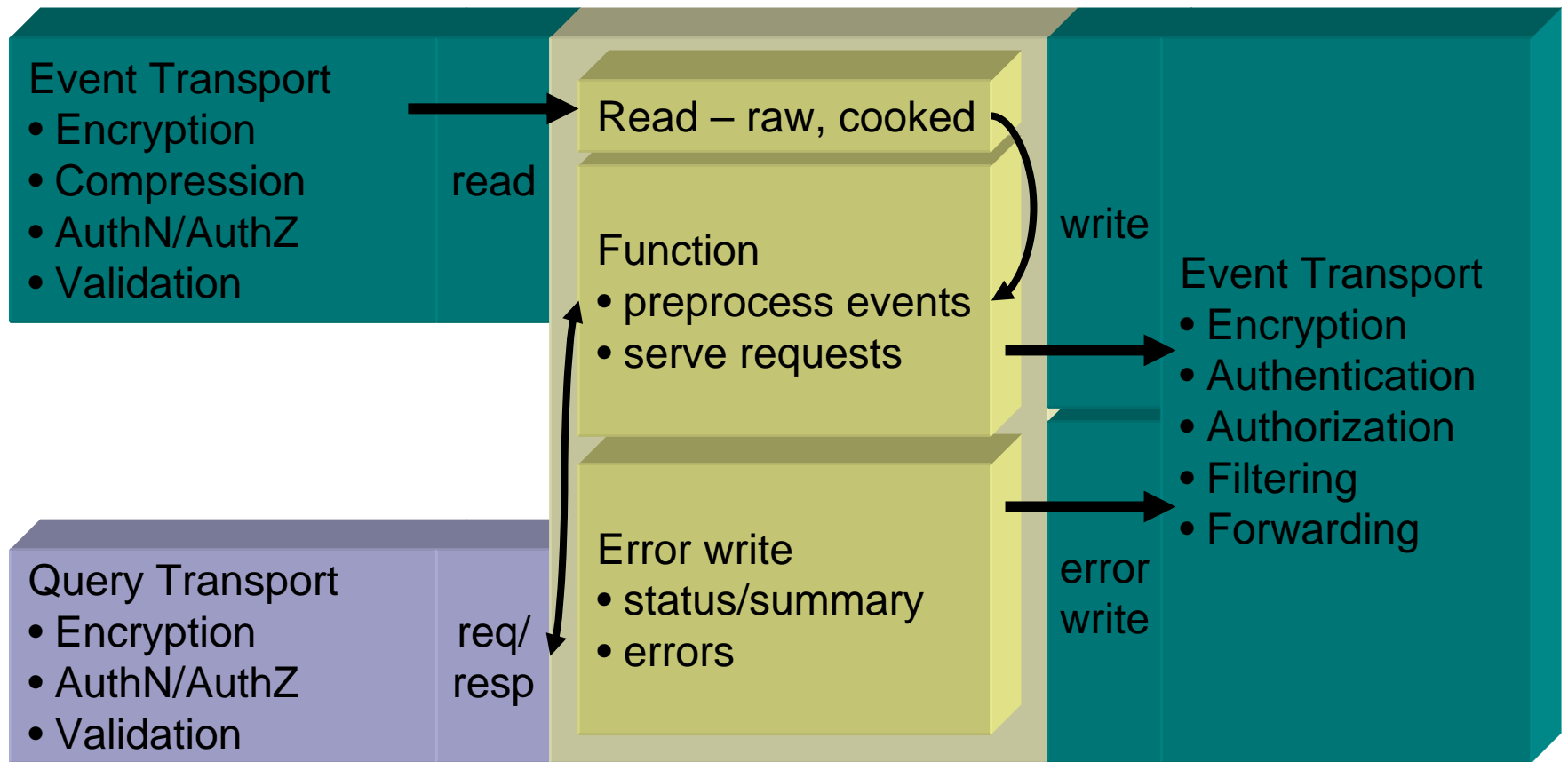


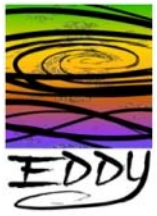
Display (read)

- Function
 - Read from the event channel and preprocess event data for visualization purposes
 - Serve requests from display consoles
 - Function can be specialized
 - General event feed
 - Summarization and aggregation
 - Offloading processing from display consoles

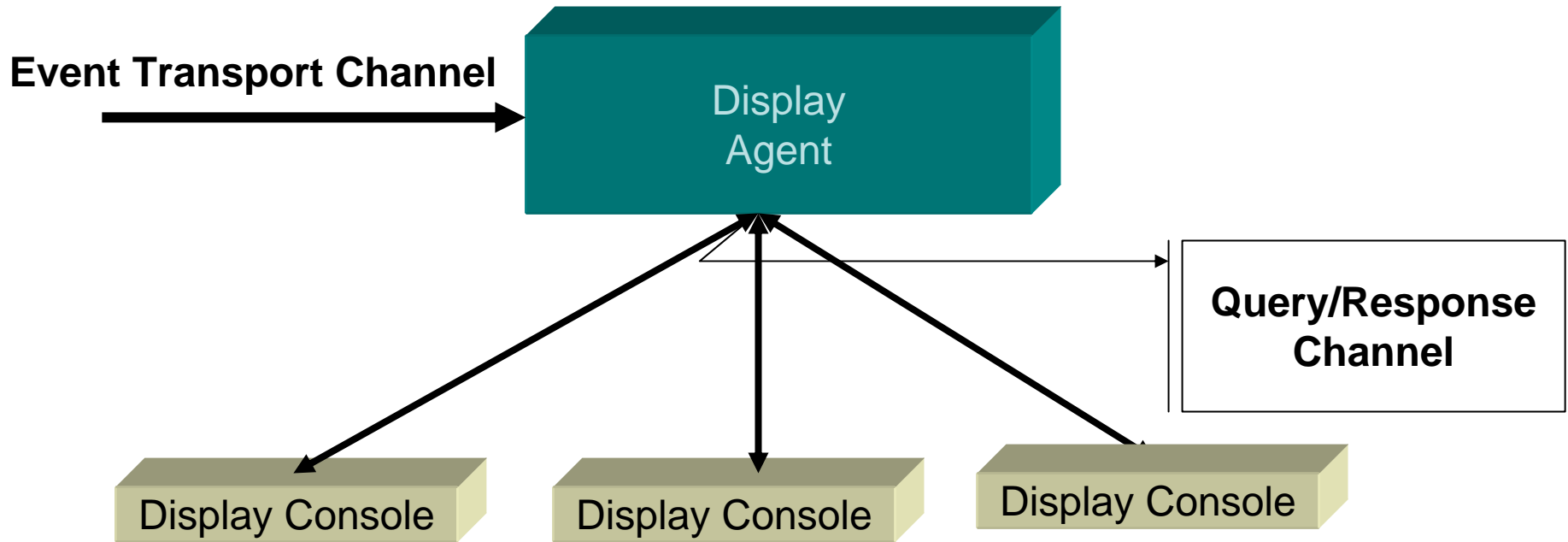


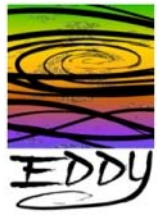
Display Agent (read/write)





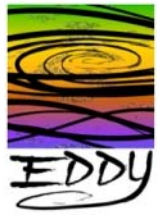
Display Agent Architecture





Event Storage Agents

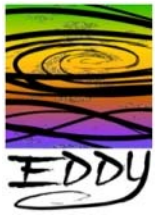
- Storage-Basic
- Storage-HP
- Directory



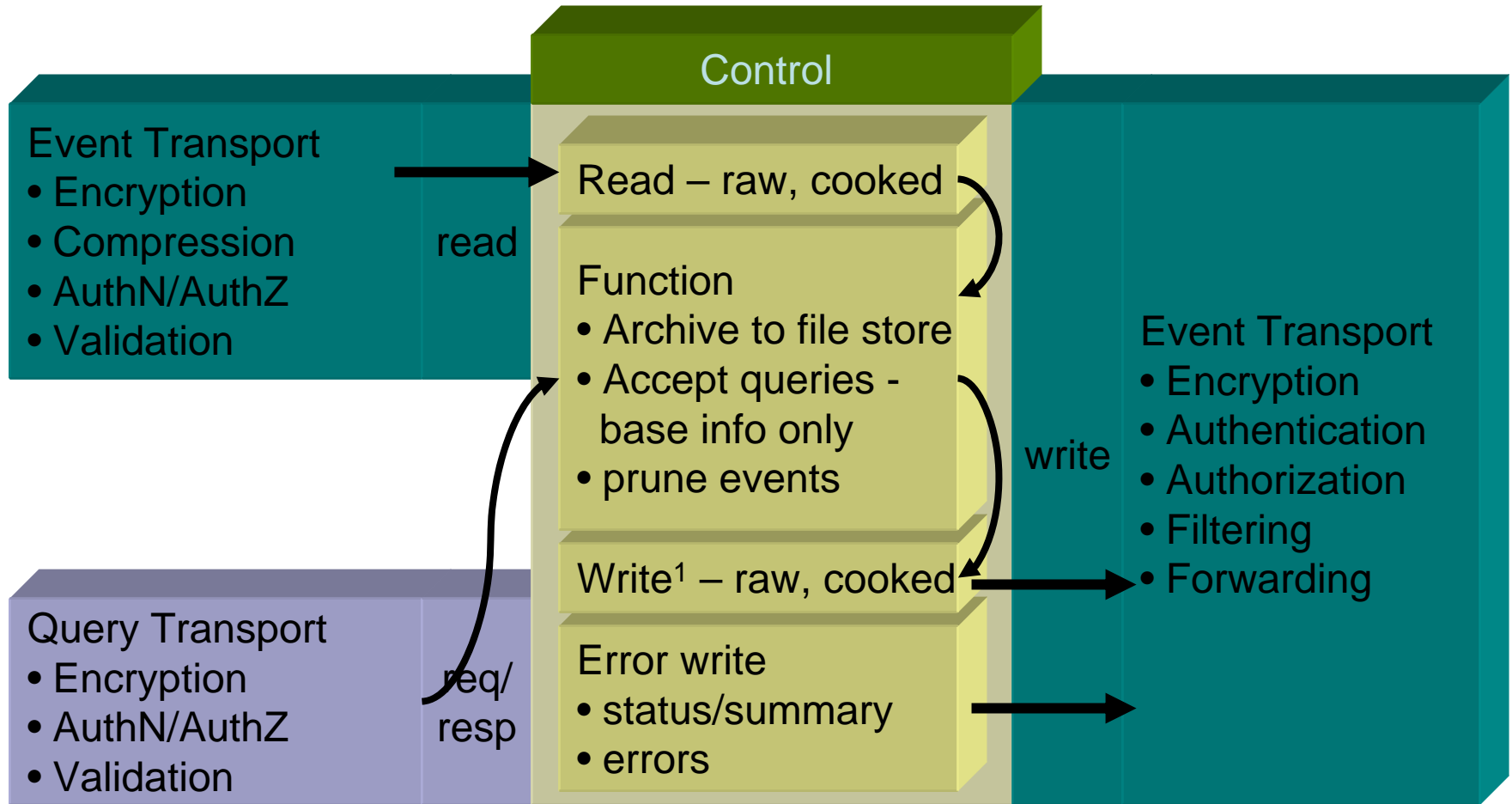
Storage-HP

Agent (read/write opt.)

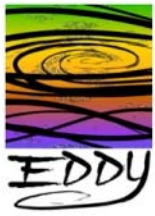
- Function
 - Read raw, cooked, or analyzed CER's from the event channel
 - Store CERs and write them to the archive file system
 - Create an index will be based on the baseInfo field of the CER
 - Accept queries on the query channel and return a CER(s) that matches the query



Storage Agent - HP (read/write opt.)

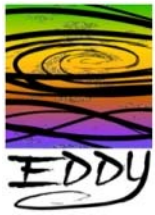


Note 1: A write to the Event transport channel is optional

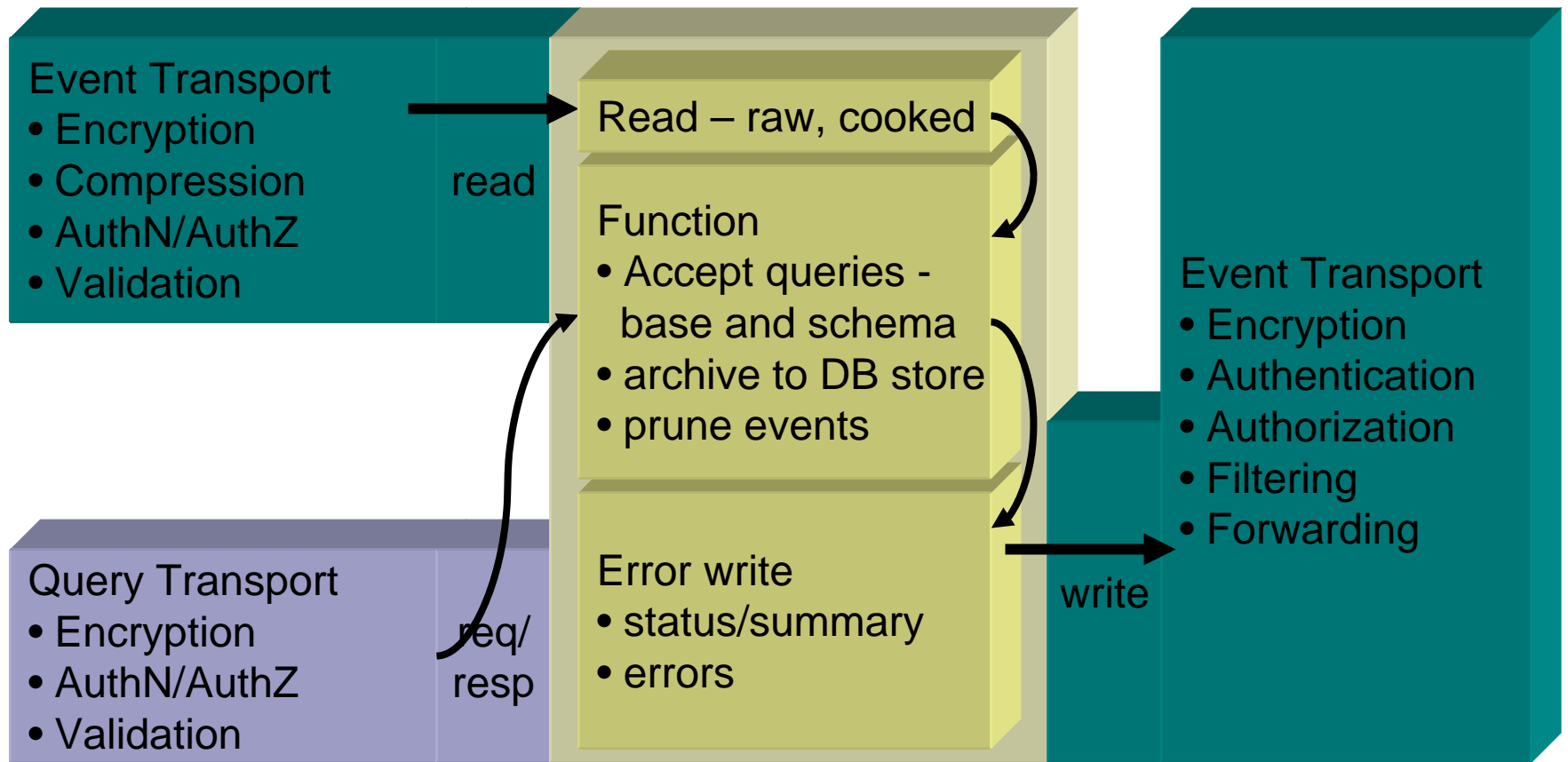


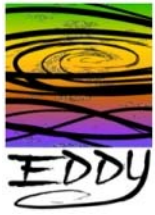
Storage Agent (read)

- Function
 - Read raw, cooked, or analyzed CER's from the event channel
 - Store CERs and write them to the DB based on a predetermined schema
 - Accept queries on the query channel and return a specific record that matches the query



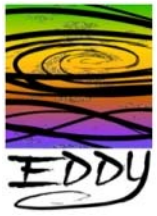
Storage Agent (read)



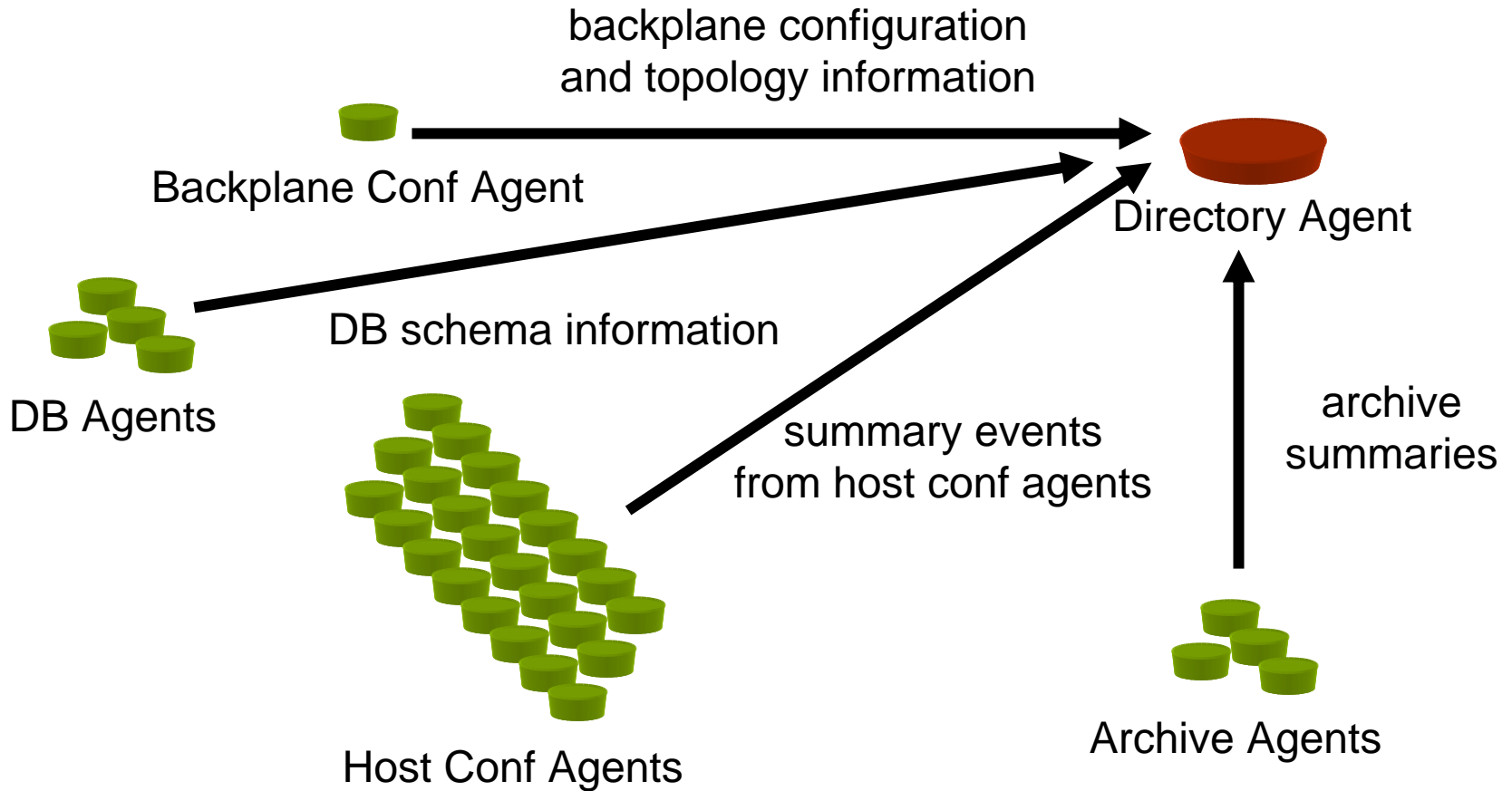


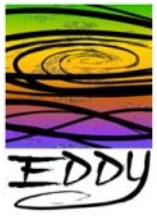
Directory Agent (read/write opt.)

- Function
 - Read cooked summary CER's from the following agents
 - Host-configuration and Backplane-configuration
 - DB and Archive
 - Create an index from summaries to assist locating specific event data
 - Accept queries on the query channel and return a specific resource (agent) that matches the query

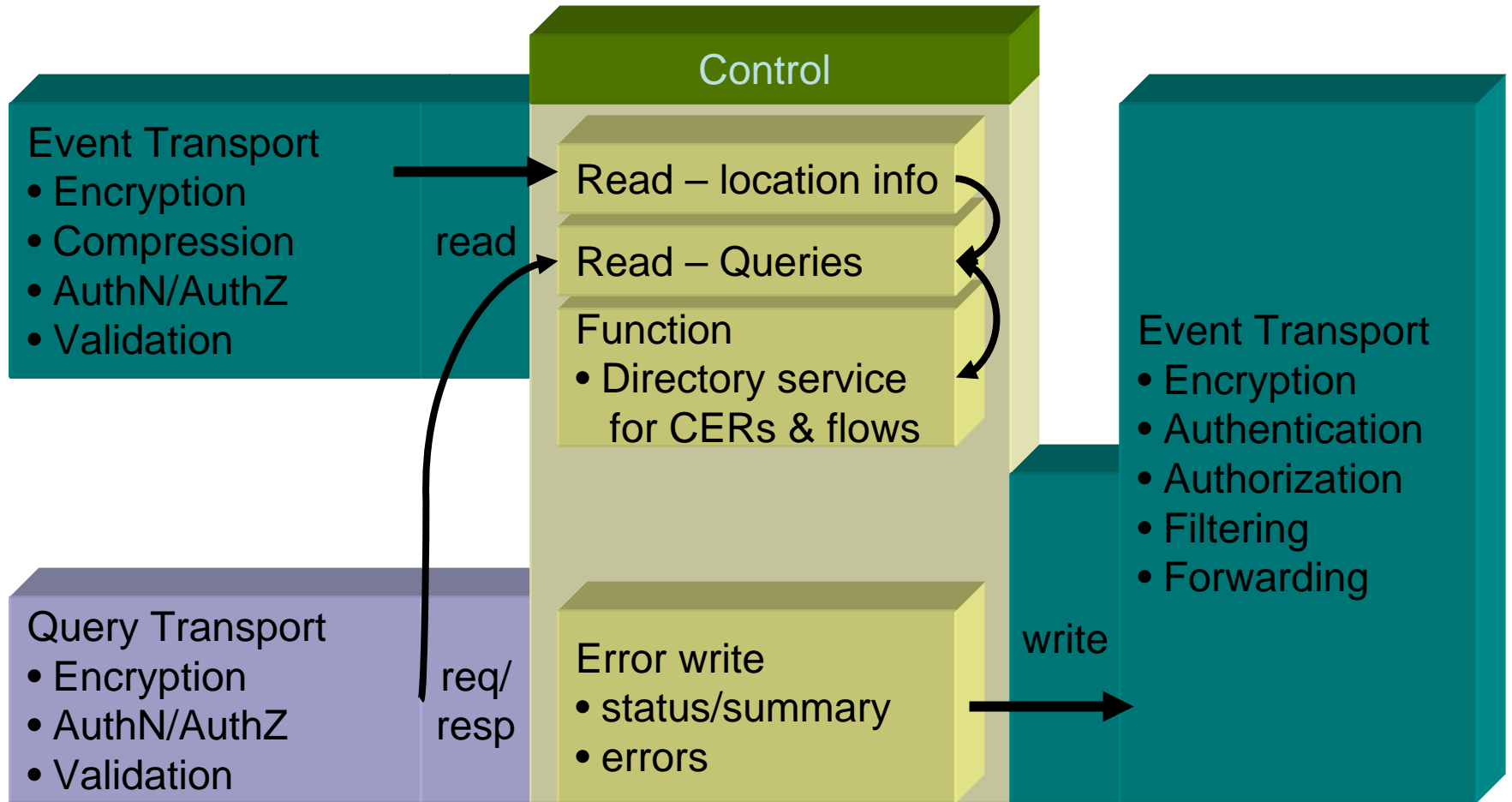


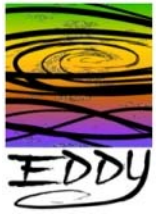
Directory Agent Functionality





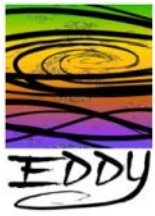
Directory Agent (read/write opt.)





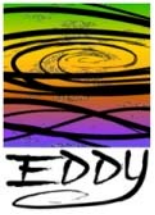
Backplane Control Agents

- Backplane Manager
- Agent Manager

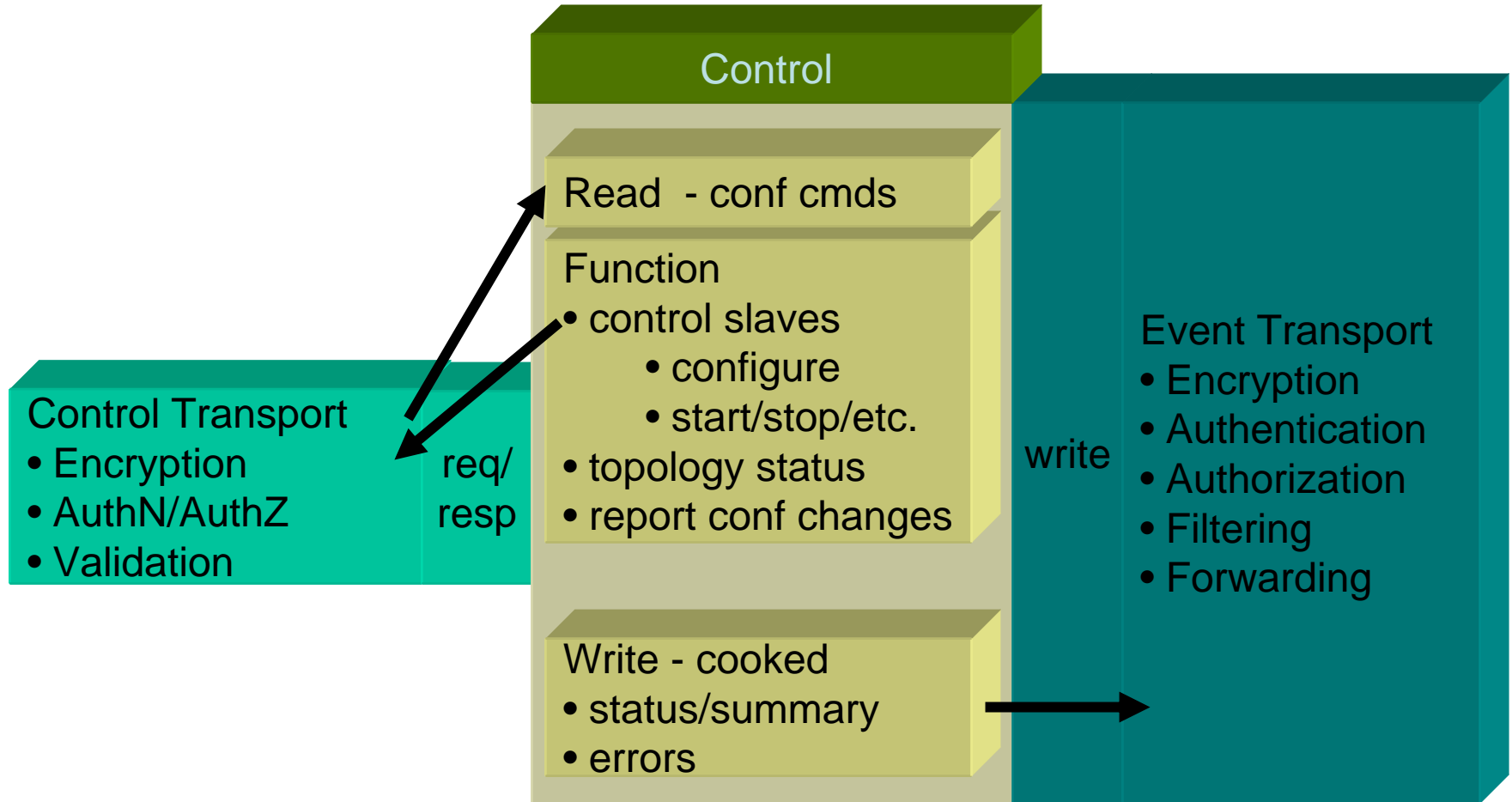


Backplane Manager

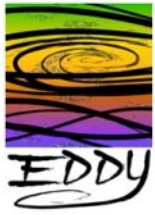
- Function
 - Accept commands from control channel to configure backplane
 - Communicate with agent manager to control specific agents
 - Write configuration related events that were performed into the event channel of the backplane



Backplane Manager

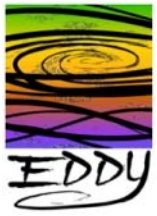


Note: All read and write components have multiple sources and destinations

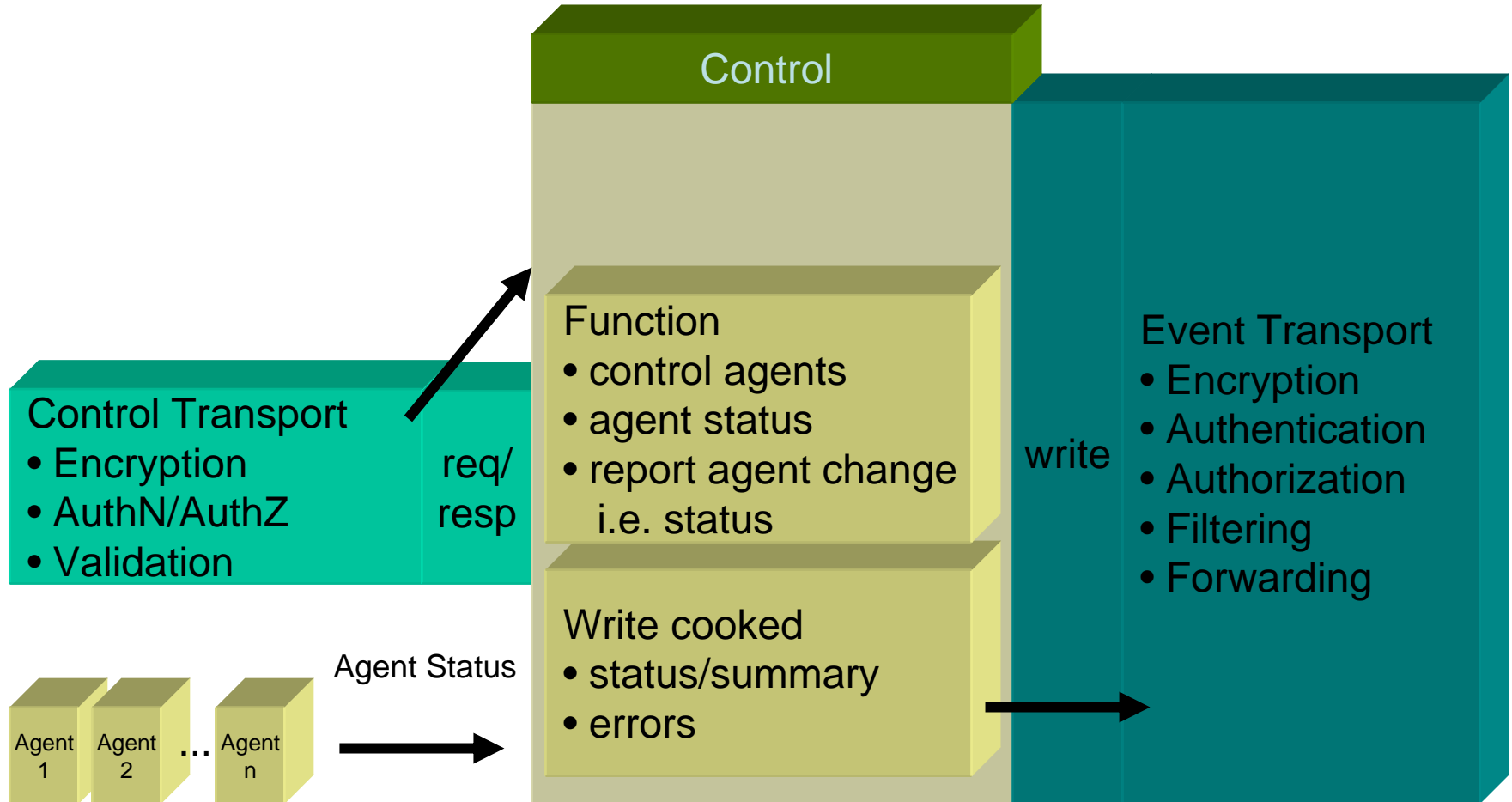


Agent Manager

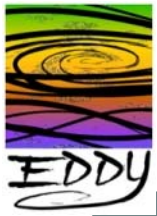
- Function
 - Communicate with local agents for control (start, stop, restart)
 - Accept commands from backplane configuration agent on the control channel for configuring agents on host
 - Read event channel events and forward to appropriate local agents
 - Write configuration related events that were performed into the event channel of the backplane



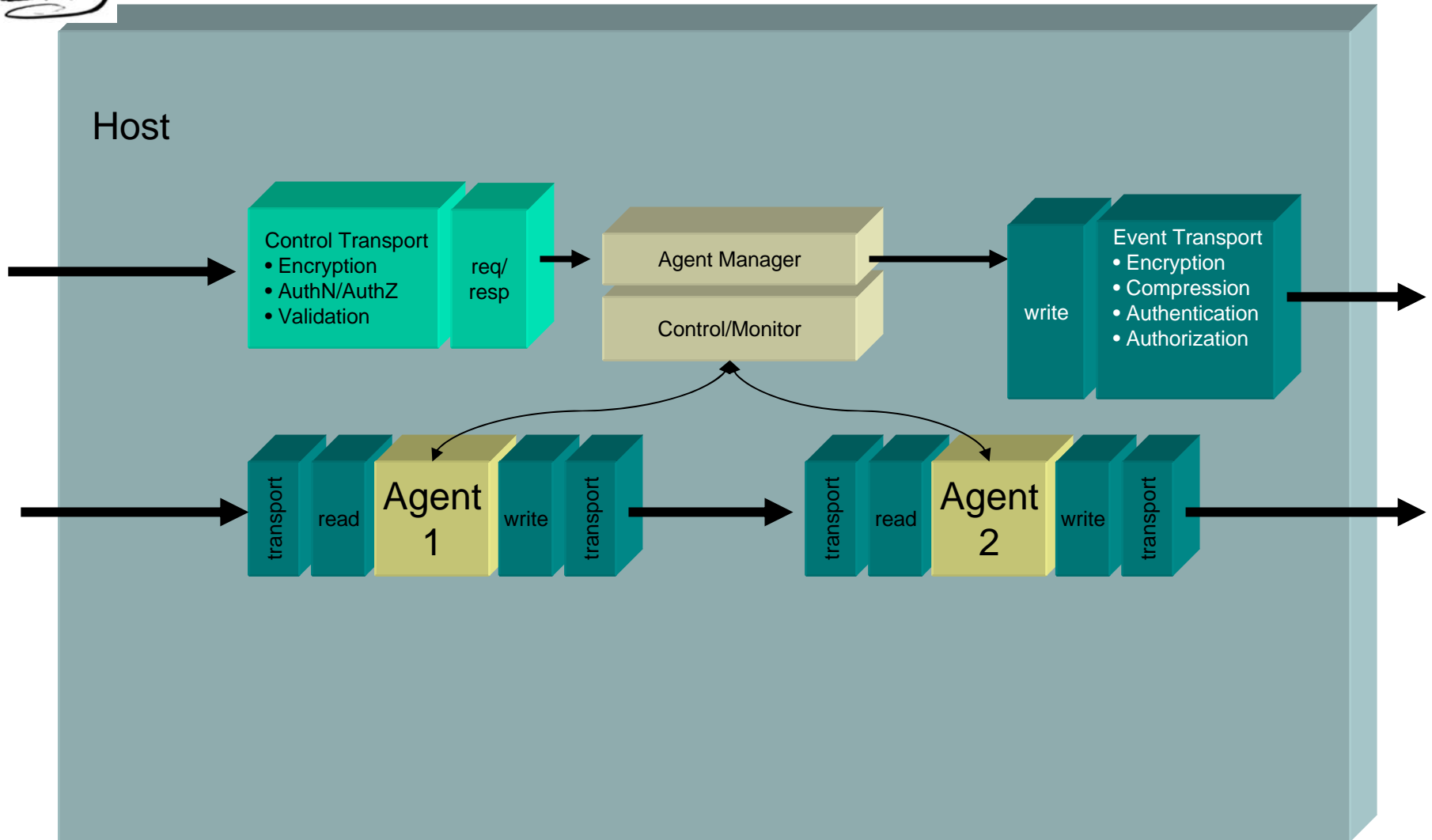
Agent Manager

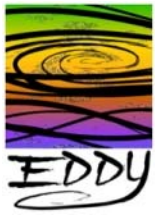


Note: All read and write components have multiple sources and destinations



Agent Manager





Master Configuration Agent

