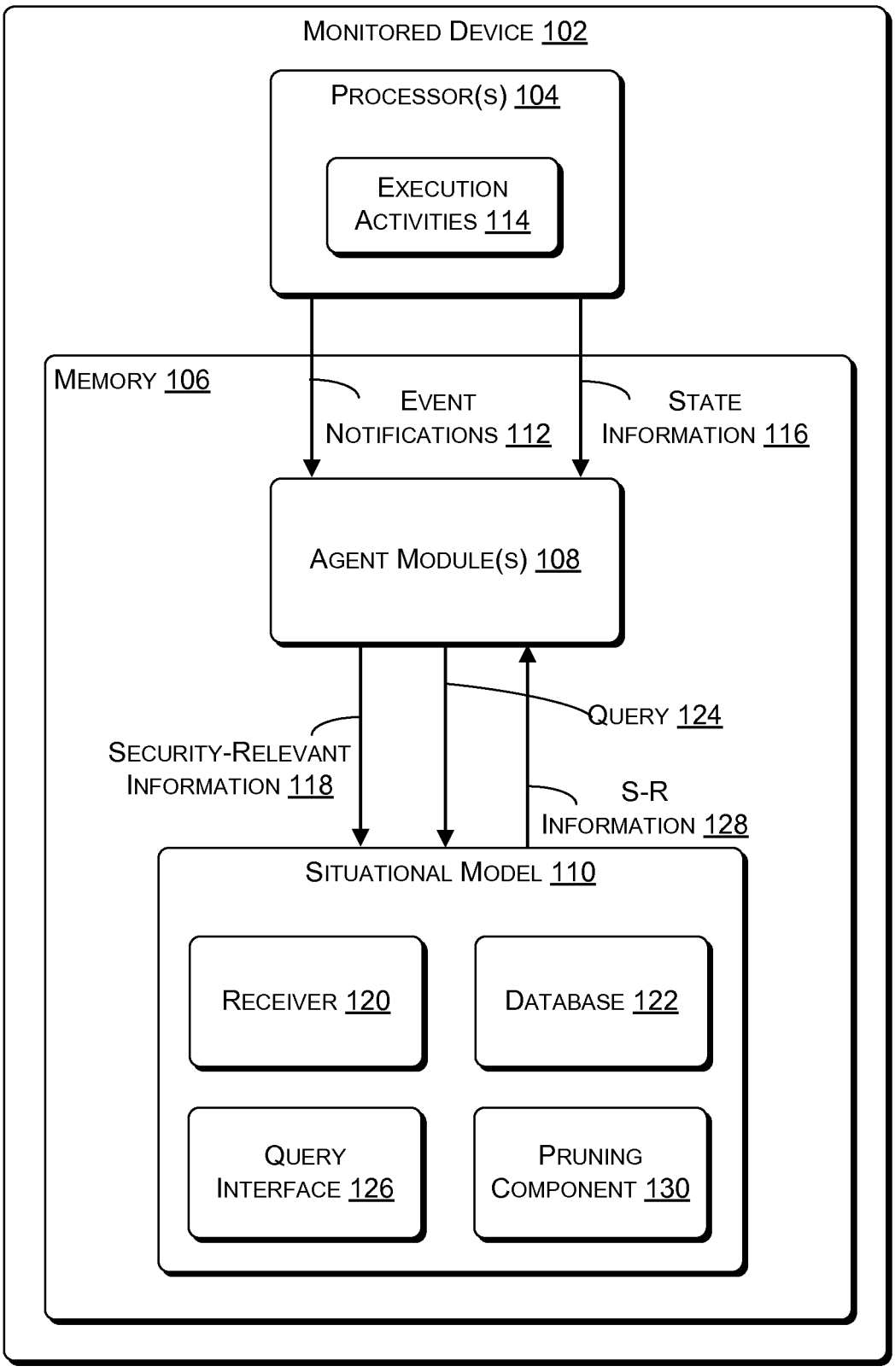
MONITORED DEVICE 102
PROCESSOR(S) 104
EXECUTION ACTIVITIES 114
MEMORY 106
EVENT NOTIFICATIONS 112
STATE INFORMATION 116
AGENT MODULE(S) 108
QUERY 124
SECURITY-RELEVANT INFORMATION 118
S-R INFORMATION 128
SITUATIONAL MODEL 110
RECEIVER 120
DATABASE 122
QUERY INTERFACE 126
PRUNING COMPONENT 130

Fig. 1

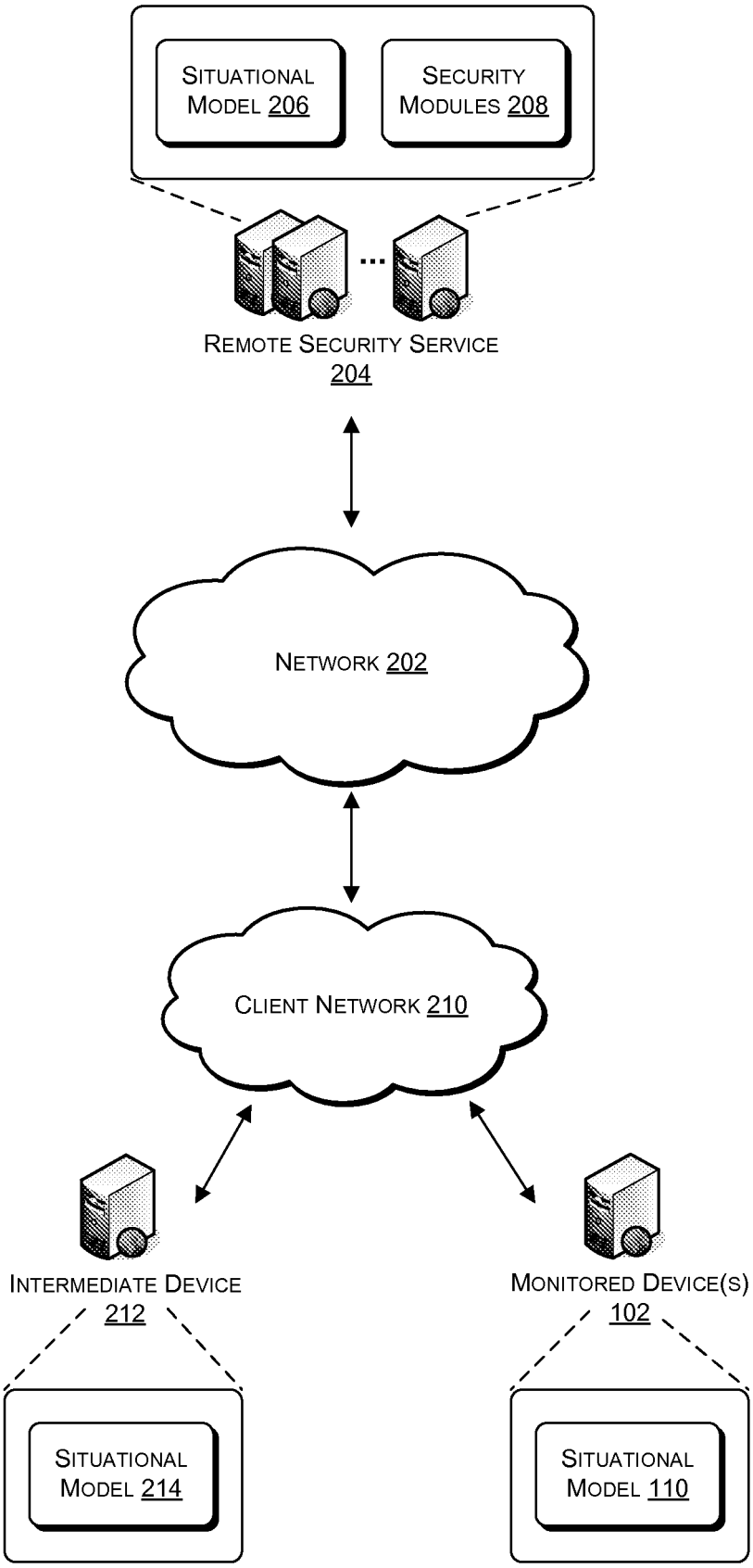
SITUATIONAL MODEL 206
SECURITY MODULES 208
REMOTE SECURITY SERVICE 204
NETWORK 202
CLIENT NETWORK 210
INTERMEDIATE DEVICE 212
MONITORED DEVICE(S) 102
SITUATIONAL MODEL 214
SITUATIONAL MODEL 110

Fig. 2

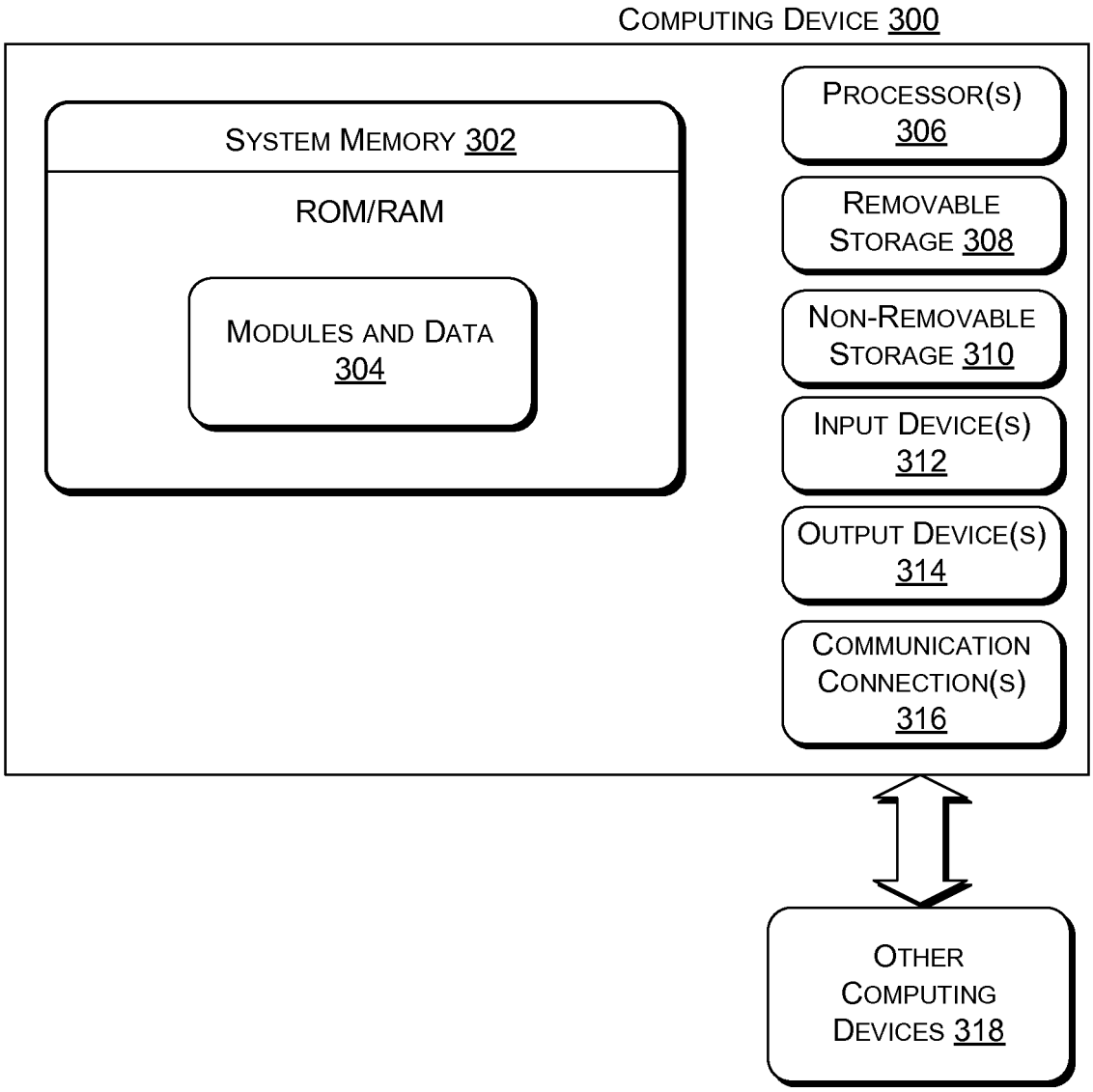
COMPUTING DEVICE 300
SYSTEM MEMORY 302
ROM/RAM
MODULES AND DATA 304
PROCESSOR(S) 306
REMOVABLE STORAGE 308
NON-REMOVABLE STORAGE 310
INPUT DEVICE(S) 312
OUTPUT DEVICE(S) 314
COMMUNICATION CONNECTION(S) 316
OTHER COMPUTING DEVICES 318

FIG. 3

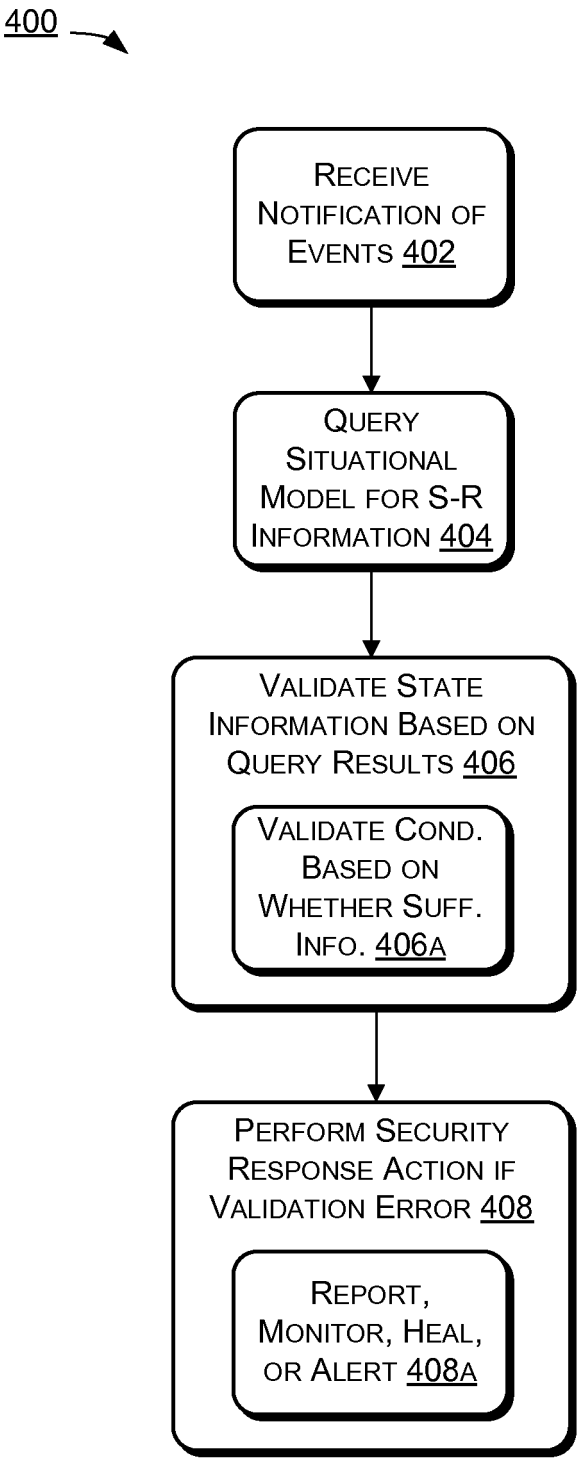
400
RECEIVE NOTIFICATION OF EVENTS 402
QUERY SITUATIONAL MODEL FOR S-R INFORMATION 404
VALIDATE STATE INFORMATION BASED ON QUERY RESULTS 406
VALIDATE COND. BASED ON WHETHER SUFF. INFO. 406A
PERFORM SECURITY RESPONSE ACTION IF VALIDATION ERROR 408
REPORT, MONITOR, HEAL, OR ALERT 408A

FIG. 4

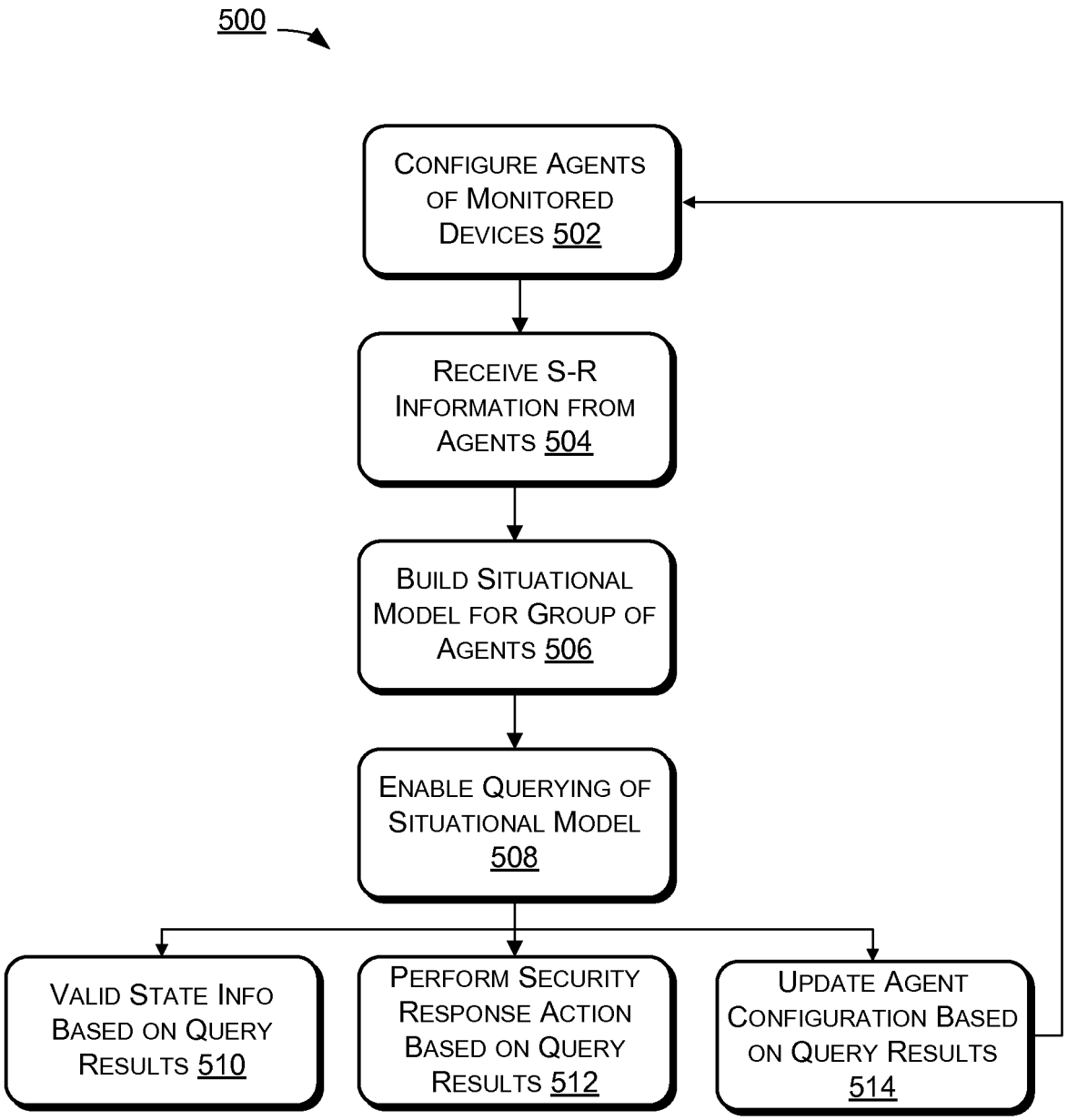
500
CONFIGURE AGENTS OF MONITORED DEVICES 502
RECEIVE S-R INFORMATION FROM AGENTS 504
BUILD SITUATIONAL MODEL FOR GROUP OF AGENTS 506
ENABLE QUERYING OF SITUATIONAL MODEL 508
VALID STATE INFO BASED ON QUERY RESULTS 510
PERFORM SECURITY RESPONSE ACTION BASED ON QUERY RESULTS 512
UPDATE AGENT CONFIGURATION BASED ON QUERY RESULTS 514

FIG. 5