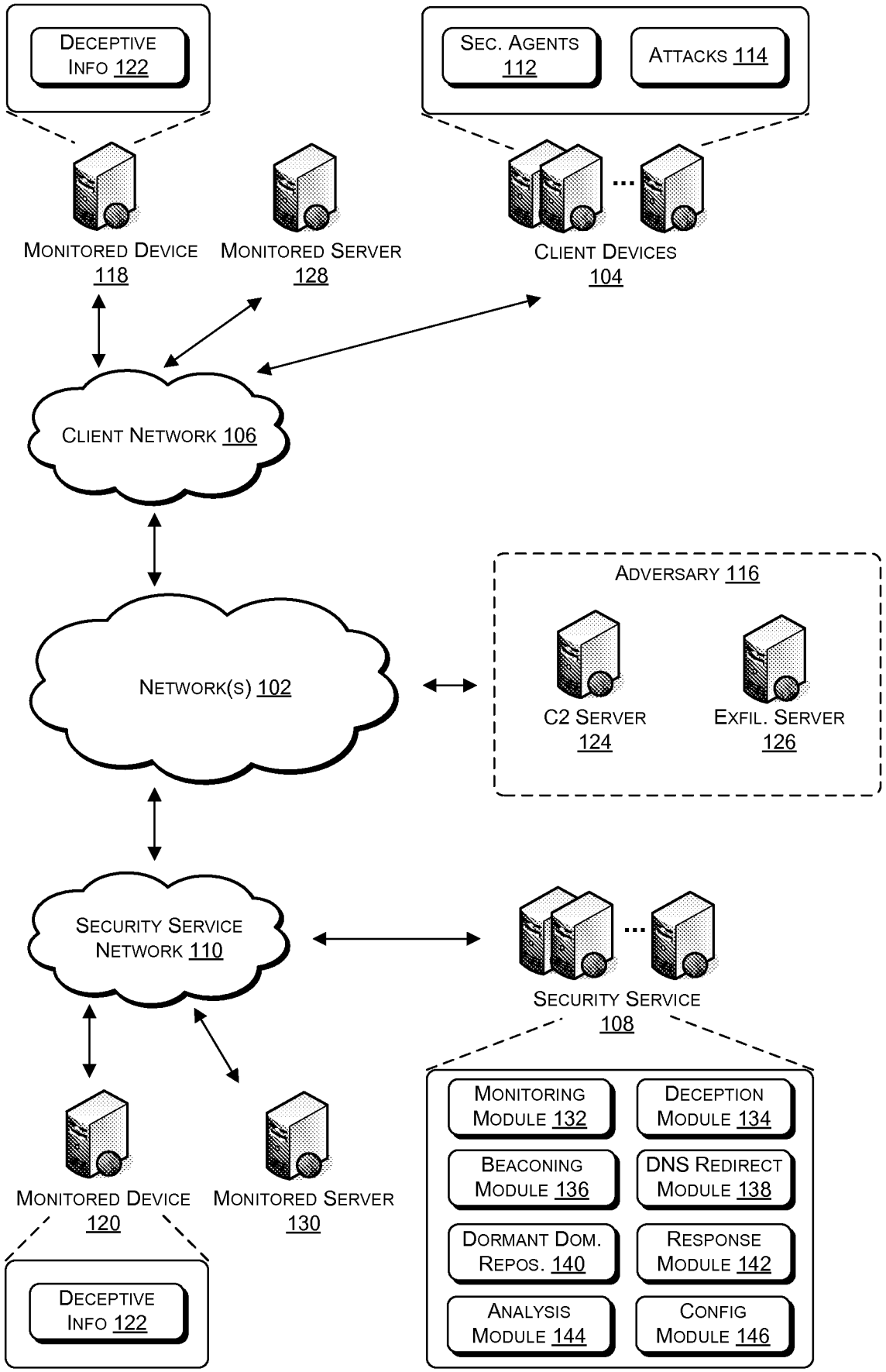
DECEPTIVE INFO 122
SEC. AGENTS 112
ATTACKS 114
MONITORED DEVICE 118
MONITORED SERVER 128
CLIENT DEVICES 104
CLIENT NETWORK 106
ADVERSARY 116
NETWORK(S) 102
C2 SERVER 124
EXFIL. SERVER 126
SECURITY SERVICE NETWORK 110
SECURITY SERVICE 108
MONITORING MODULE 132
DECEPTION MODULE 134
BEACONING MODULE 136
DNS REDIRECT MODULE 138
DORMANT DOM. REPOS. 140
RESPONSE MODULE 142
ANALYSIS MODULE 144
CONFIG MODULE 146
MONITORED DEVICE 120
MONITORED SERVER 130
DECEPTIVE INFO 122

Fig. 1

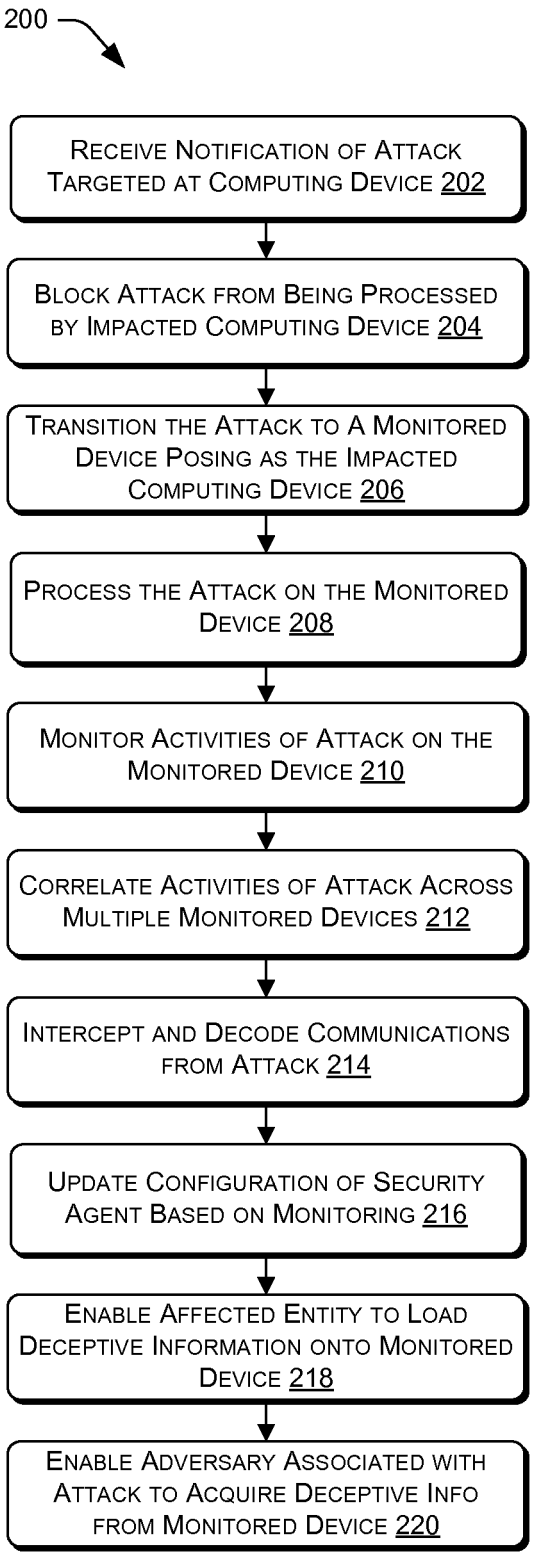
200
Receive Notification of Attack Targeted at Computing Device 202
Block Attack from Being Processed by Impacted Computing Device 204
Transition the Attack to A Monitored Device Posing as the Impacted Computing Device 206
Process the Attack on the Monitored Device 208
Monitor Activities of Attack on the Monitored Device 210
Correlate Activities of Attack Across Multiple Monitored Devices 212
Intercept and Decode Communications from Attack 214
Update Configuration of Security Agent Based on Monitoring 216
Enable Affected Entity to Load Deceptive Information onto Monitored Device 218
Enable Adversary Associated with Attack to Acquire Deceptive Info from Monitored Device 220

Fig. 2

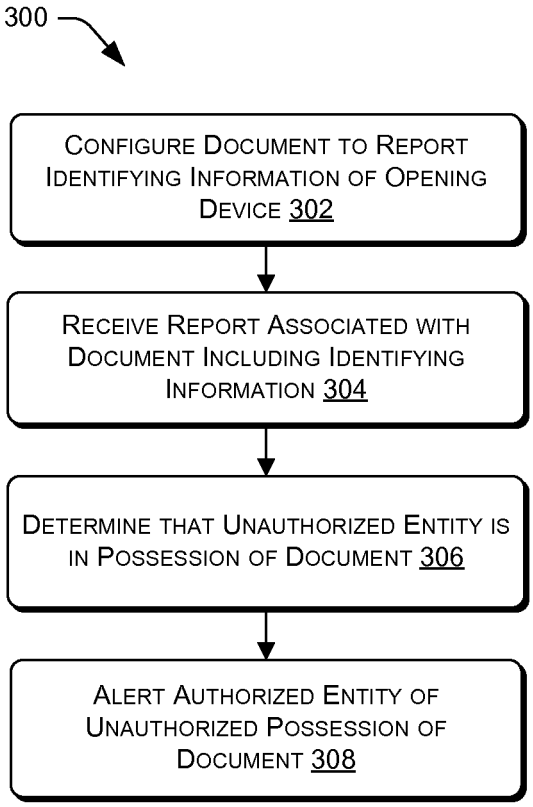
300
Configure Document to Report Identifying Information of Opening Device 302
Receive Report Associated with Document Including Identifying Information 304
Determine that Unauthorized Entity is in Possession of Document 306
Alert Authorized Entity of Unauthorized Possession of Document 308

Fig. 3

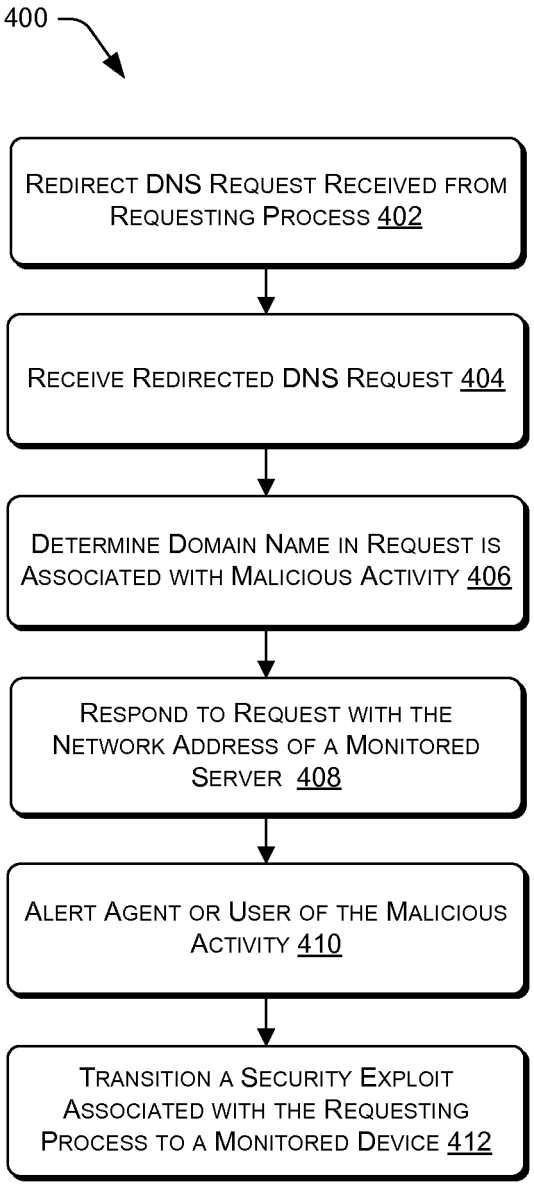
400
Redirect DNS Request Received from Requesting Process 402
Receive Redirected DNS Request 404
Determine Domain Name in Request is Associated with Malicious Activity 406
Respond to Request with the Network Address of a Monitored Server 408
Alert Agent or User of the Malicious Activity 410
Transition a Security Exploit Associated with the Requesting Process to a Monitored Device 412

Fig. 4

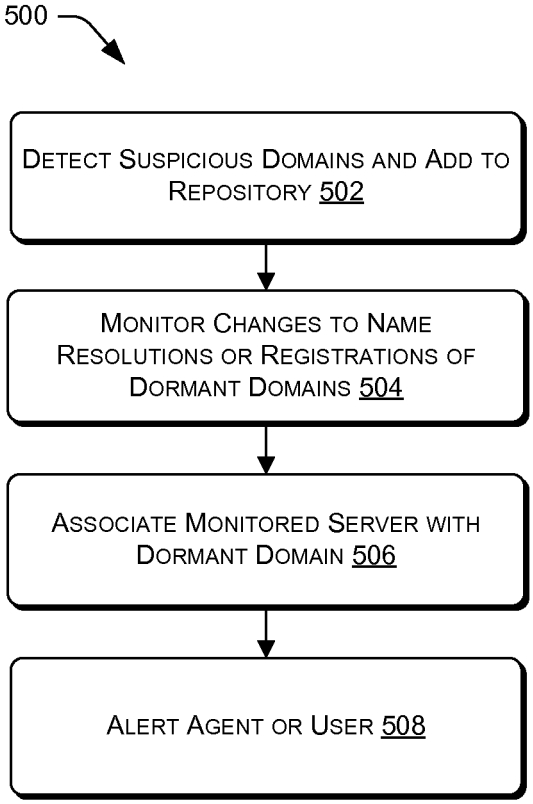
500
DETECT SUSPICIOUS DOMAINS AND ADD TO REPOSITORY 502
MONITOR CHANGES TO NAME RESOLUTIONS OR REGISTRATIONS OF DORMANT DOMAINS 504
ASSOCIATE MONITORED SERVER WITH DORMANT DOMAIN 506
ALERT AGENT OR USER 508

Fig. 5

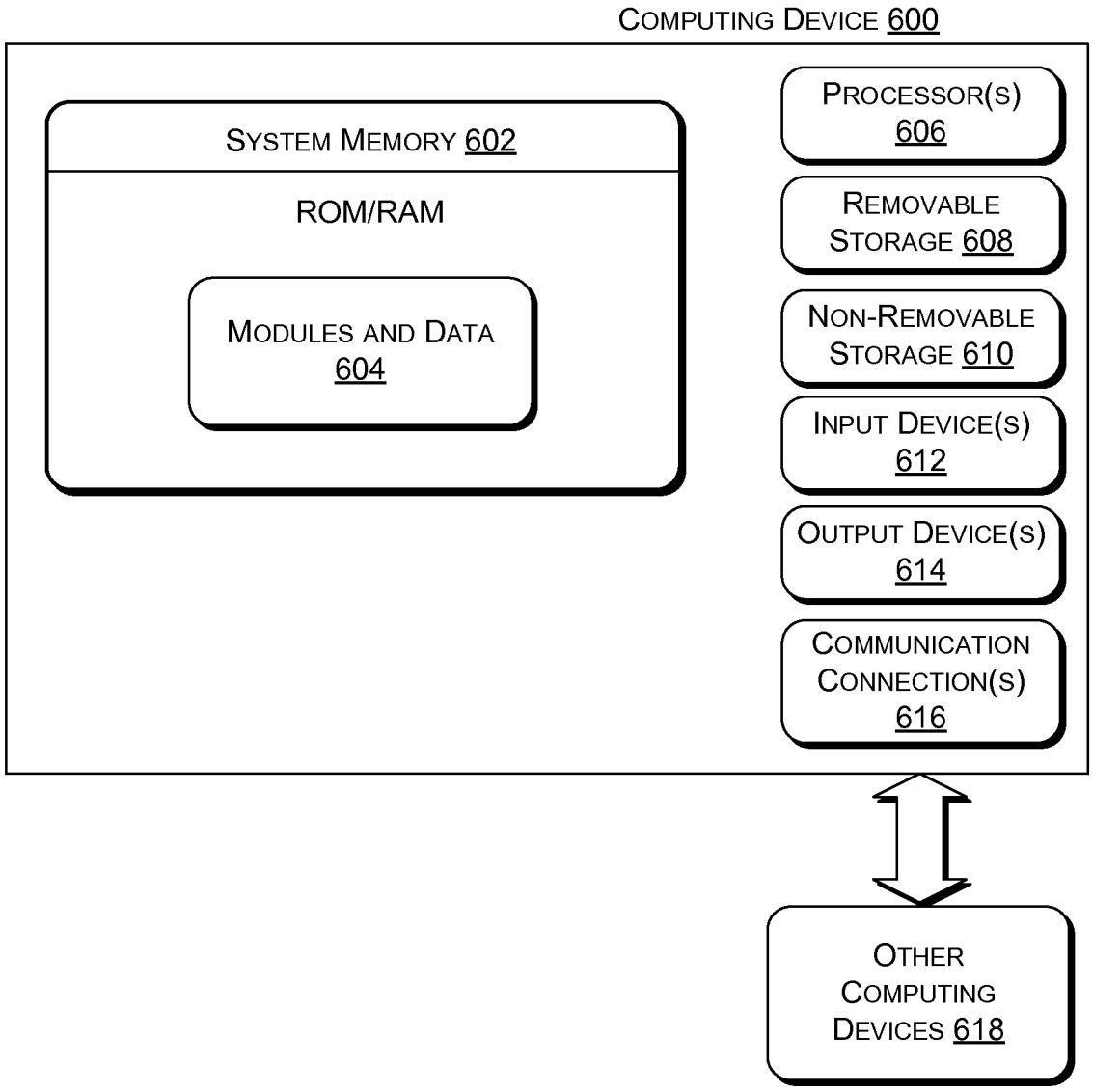
COMPUTING DEVICE 600
SYSTEM MEMORY 602
ROM/RAM
MODULES AND DATA 604
PROCESSOR(S) 606
REMOVABLE STORAGE 608
NON-REMOVABLE STORAGE 610
INPUT DEVICE(S) 612
OUTPUT DEVICE(S) 614
COMMUNICATION CONNECTION(S) 616
OTHER COMPUTING DEVICES 618

FIG. 6