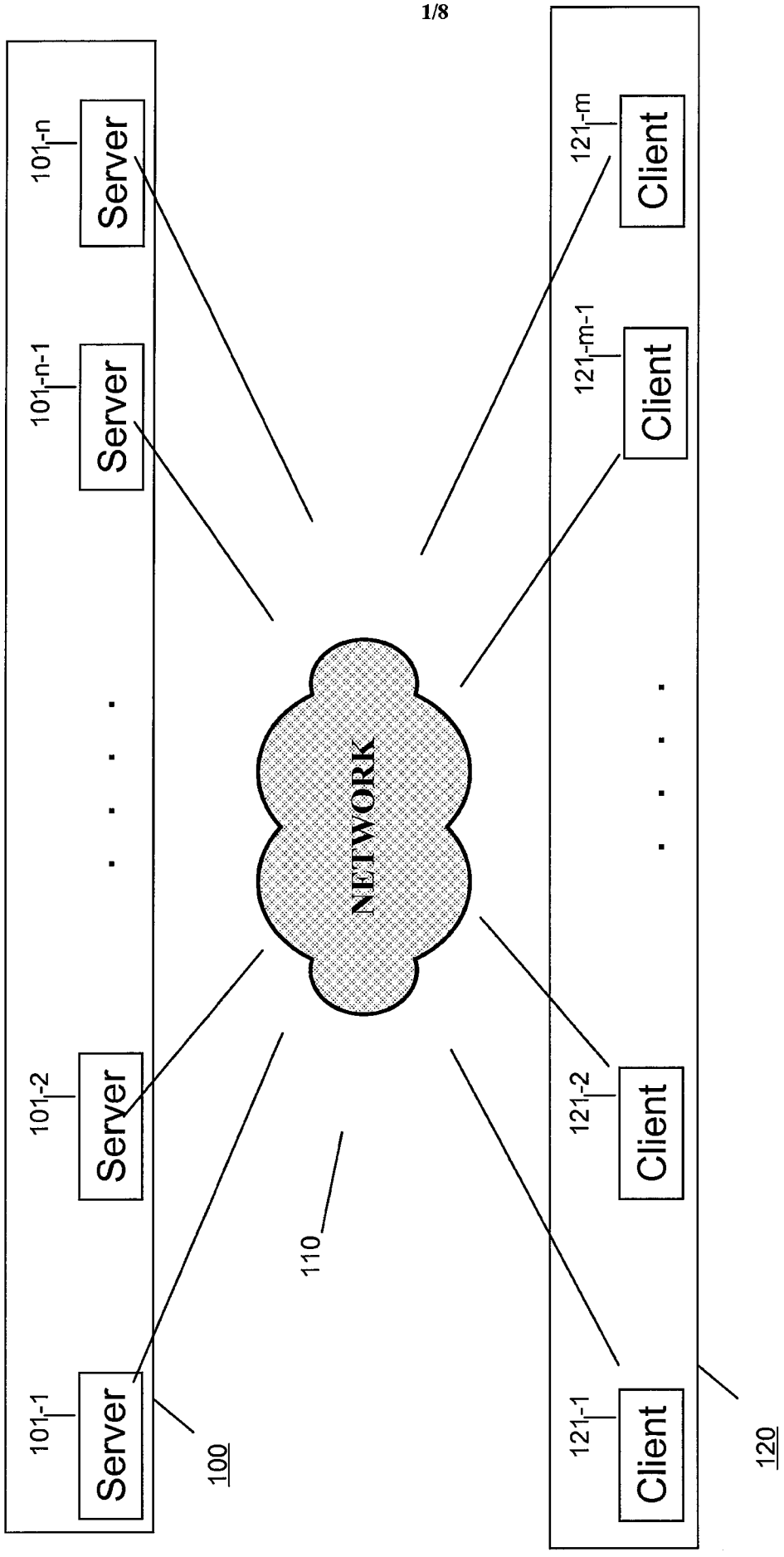
Server
Server
Server
Server
101-n
101-n-1
101-2
101-1
100
NETWORK
110
Client
Client
Client
Client
121-m
121-m-1
121-2
121-1
120

FIG. 1

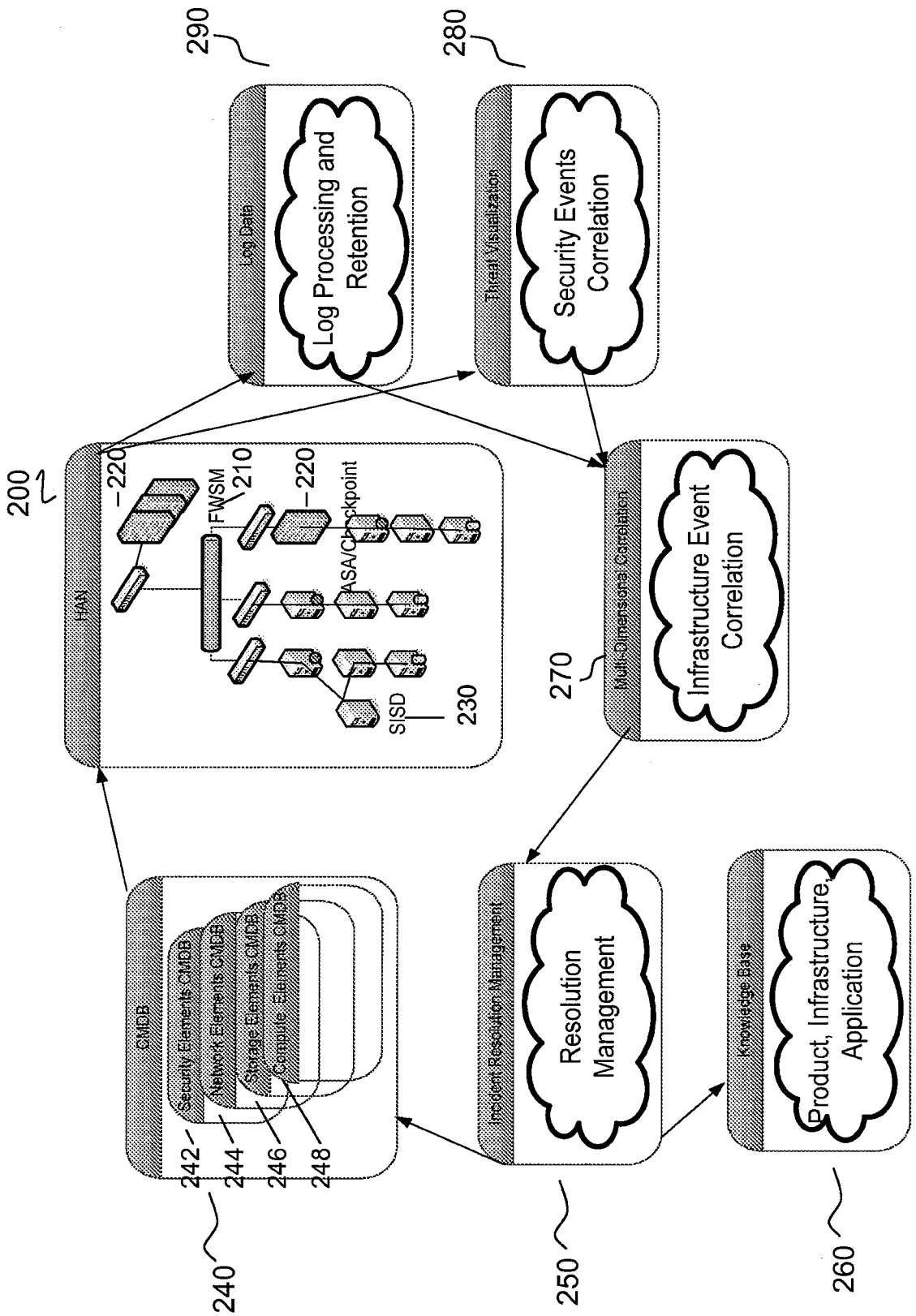
290
280
Log Data
Log Processing and Retention
Threat Visualization
Security Events Correlation
200
220
FWSM
210
220
ASA/Checkpoint
HAI
SISD
230
270
Multi-Dimensional Correlation
Infrastructure Event Correlation
CMDB
Security Elements CMDB
Network Elements CMDB
Storage Elements CMDB
Compute Elements CMDB
242
244
246
248
240
Incident Resolution Management
Resolution Management
250
Knowledge Base
Product, Infrastructure, Application
260

FIG. 2

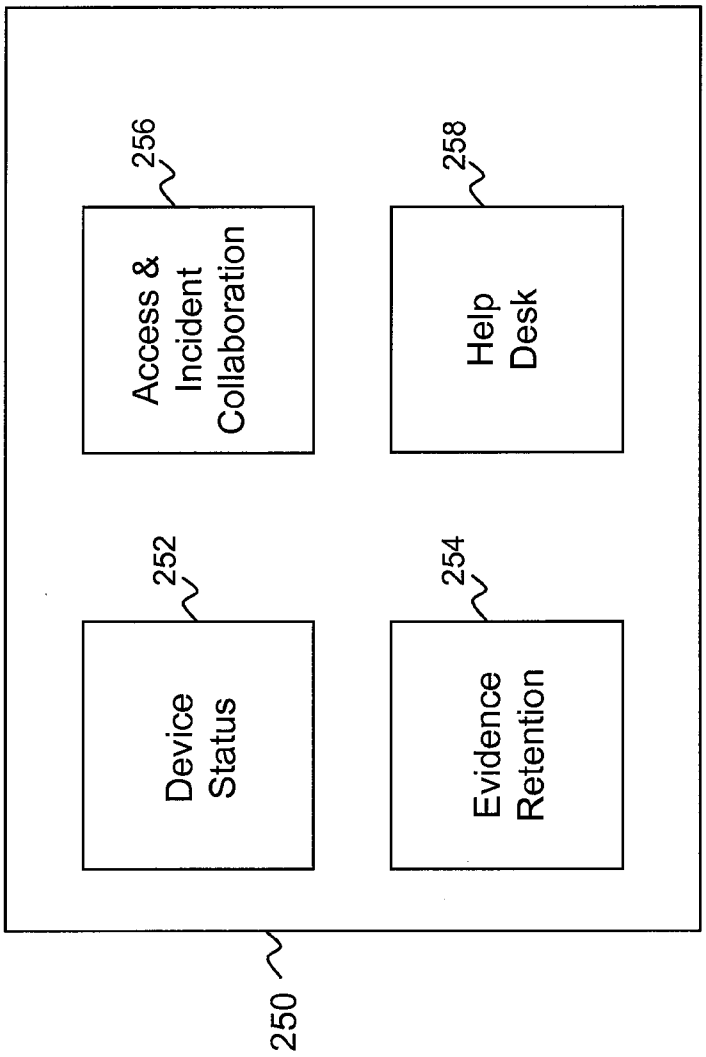
250
252
Device Status
254
Evidence Retention
256
Access & Incident Collaboration
258
Help Desk

FIG. 3

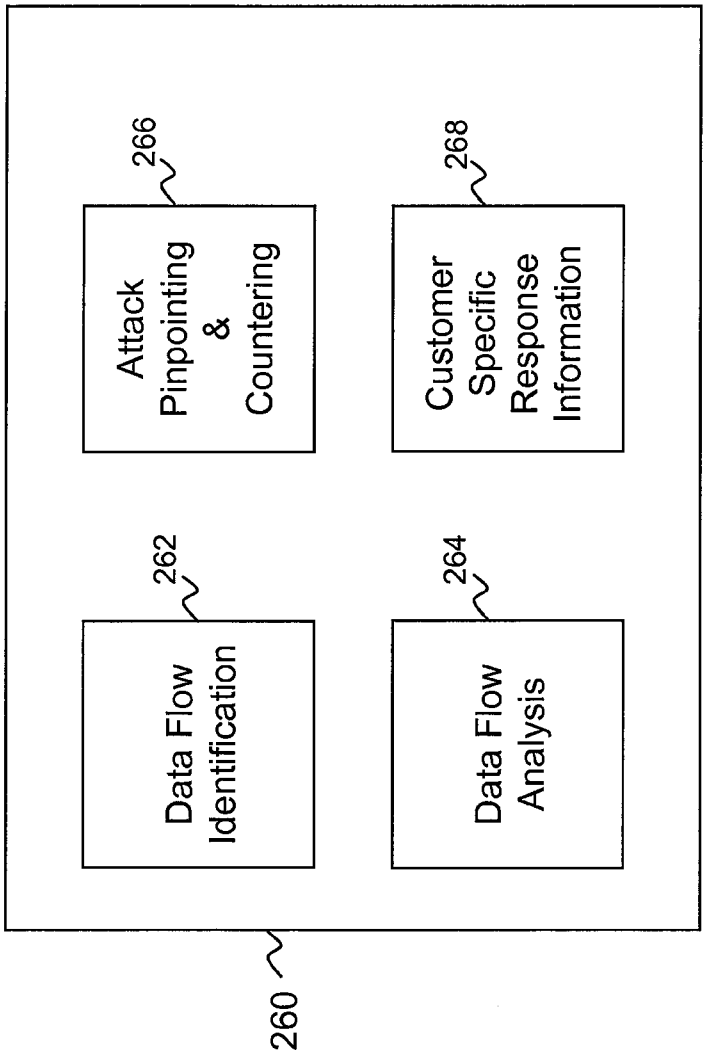
260
Data Flow Identification
262
Data Flow Analysis
264
Attack Pinpointing & Countering
266
Customer Specific Response Information
268

FIG. 4

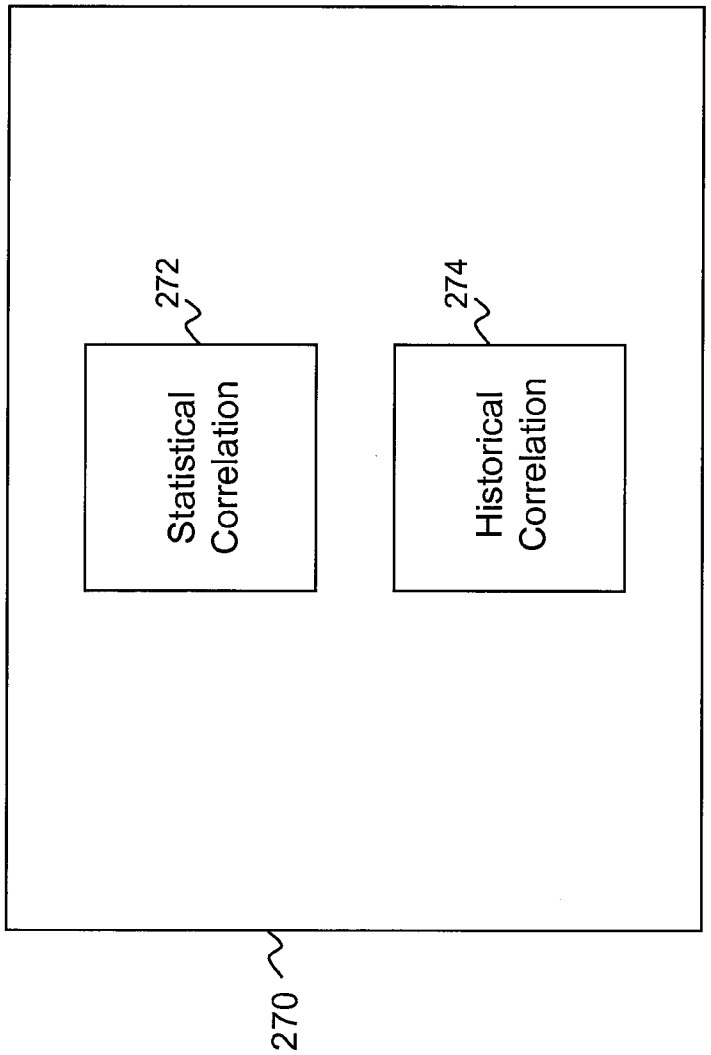
270
272
Statistical Correlation
274
Historical Correlation

FIG. 5

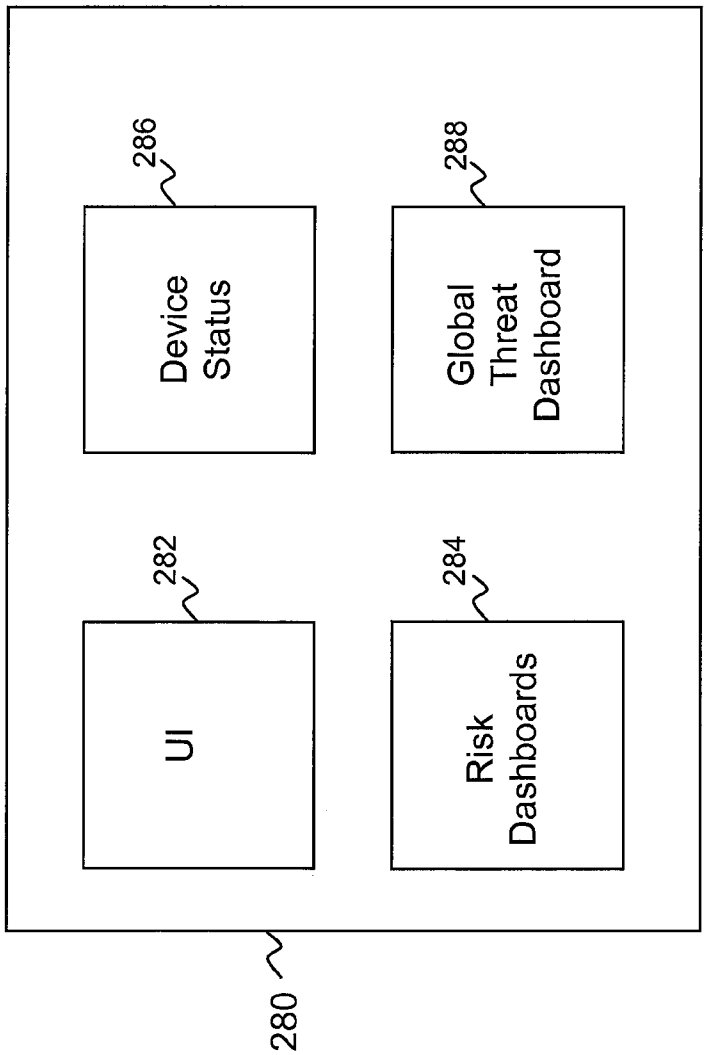
280
UI
282
Risk Dashboards
284
Device Status
286
Global Threat Dashboard
288

FIG. 6

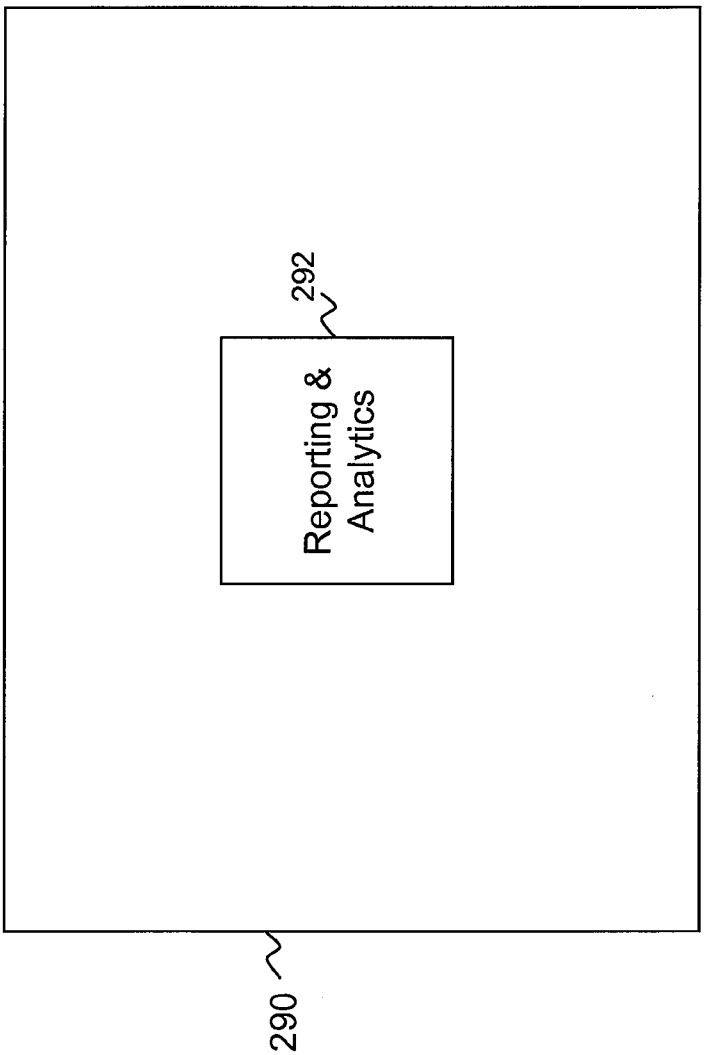

FIG. 7

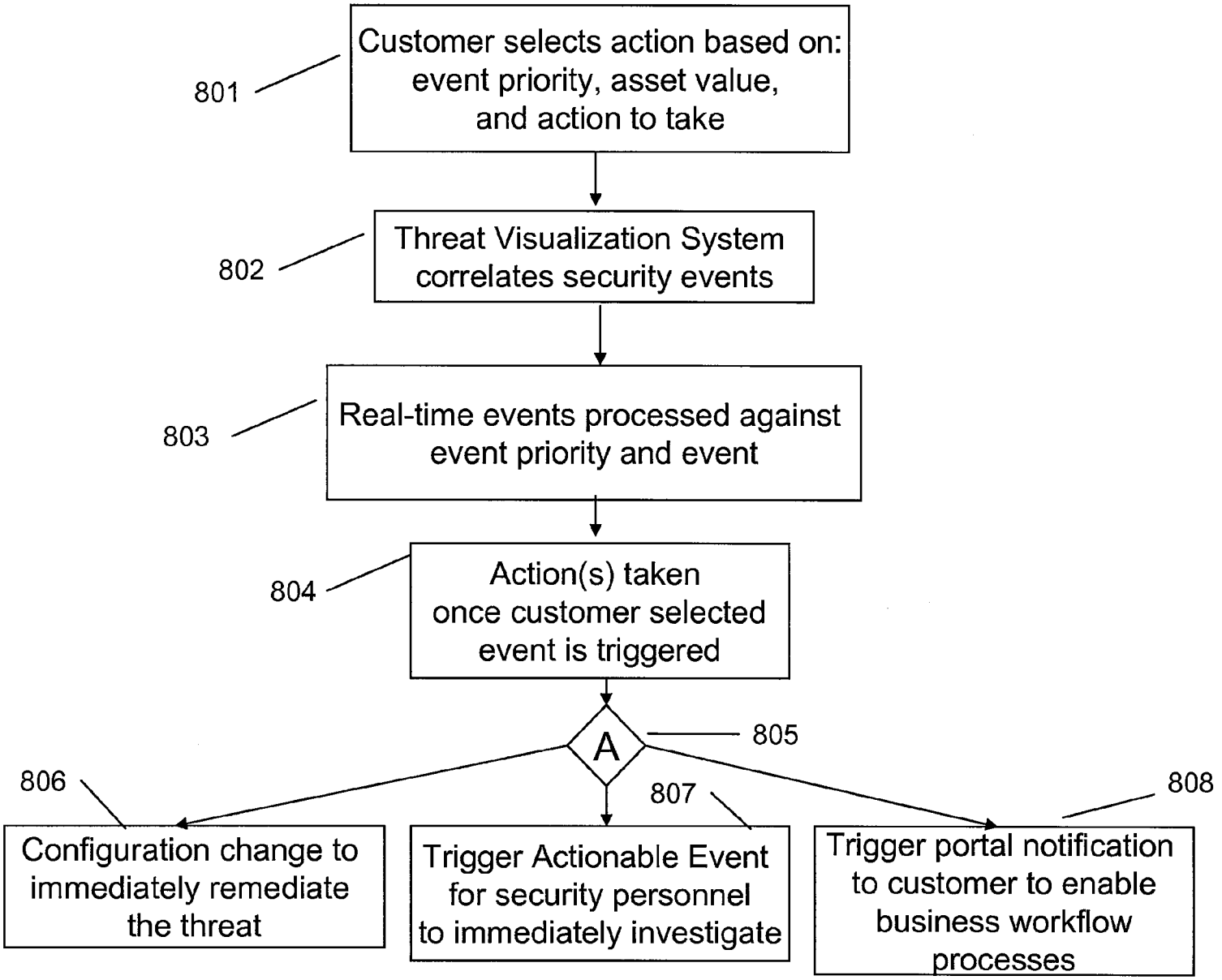
Customer selects action based on: event priority, asset value, and action to take
801
Threat Visualization System correlates security events
802
Real-time events processed against event priority and event
803
Action(s) taken once customer selected event is triggered
804
A
805
806
807
808
Configuration change to immediately remediate the threat
Trigger Actionable Event for security personnel to immediately investigate
Trigger portal notification to customer to enable business workflow processes

FIG. 8