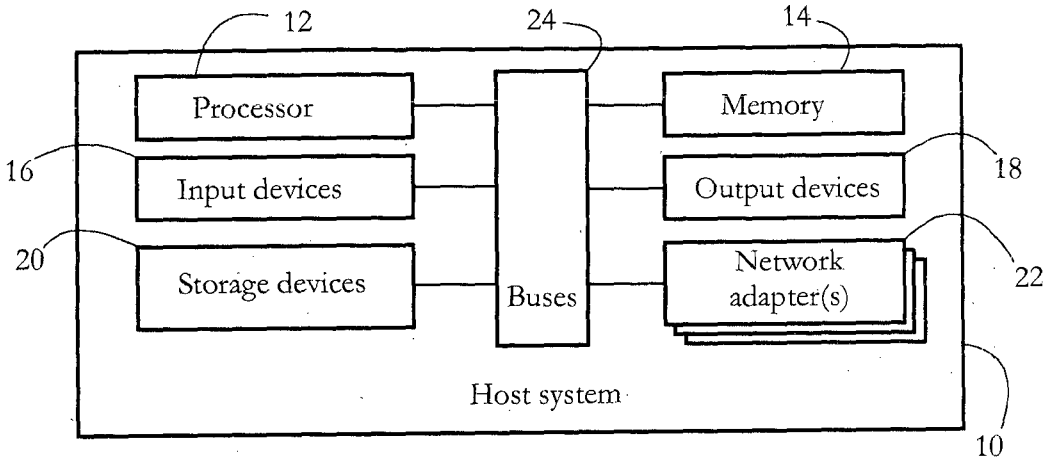
12
24
14
Processor
Memory
16
Input devices
Output devices
18
20
Storage devices
Buses
Network adapter(s)
22
Host system
10

FIG. 1

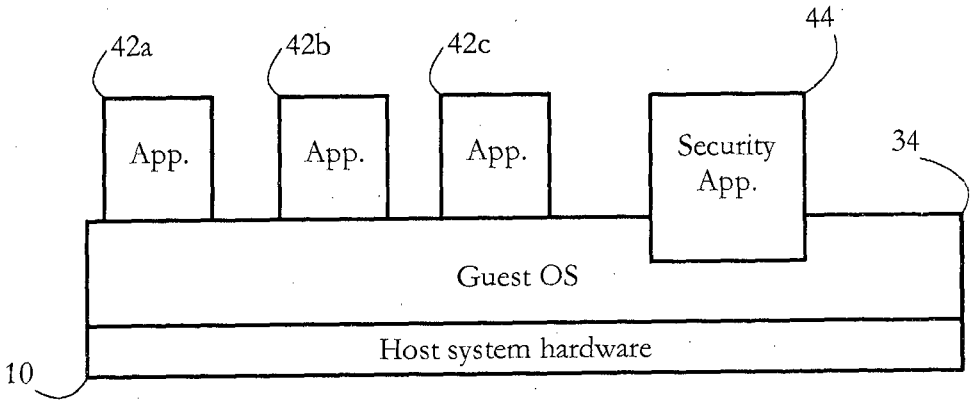
42a
42b
42c
44
App.
App.
App.
Security App.
34
Guest OS
Host system hardware
10

FIG. 2-A

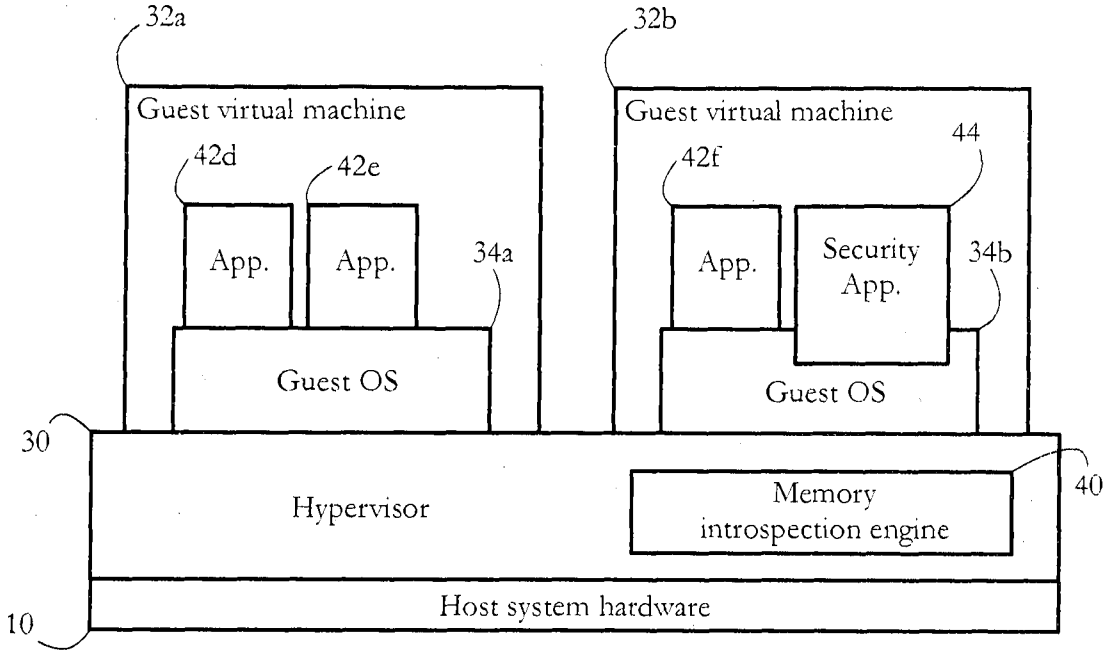
32a
32b
Guest virtual machine
Guest virtual machine
42d
42e
42f
44
App.
App.
34a
App.
Security App.
34b
Guest OS
Guest OS
30
Hypervisor
Memory introspection engine
40
Host system hardware
10

FIG. 2-B

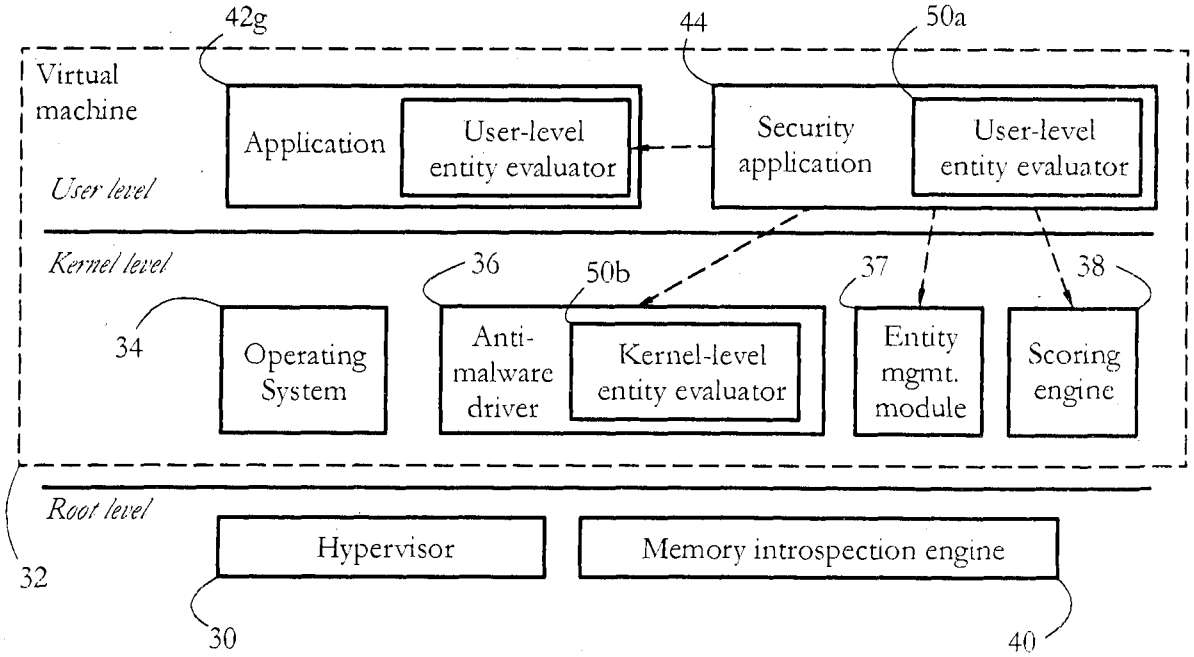
42g
44
50a
Virtual machine
Application
User-level entity evaluator
Security application
User-level entity evaluator
User level
Kernel level
36
50b
37
38
34
Operating System
Anti-malware driver
Kernel-level entity evaluator
Entity mgmt. module
Scoring engine
Root level
32
Hypervisor
Memory introspection engine
30
40

FIG. 3

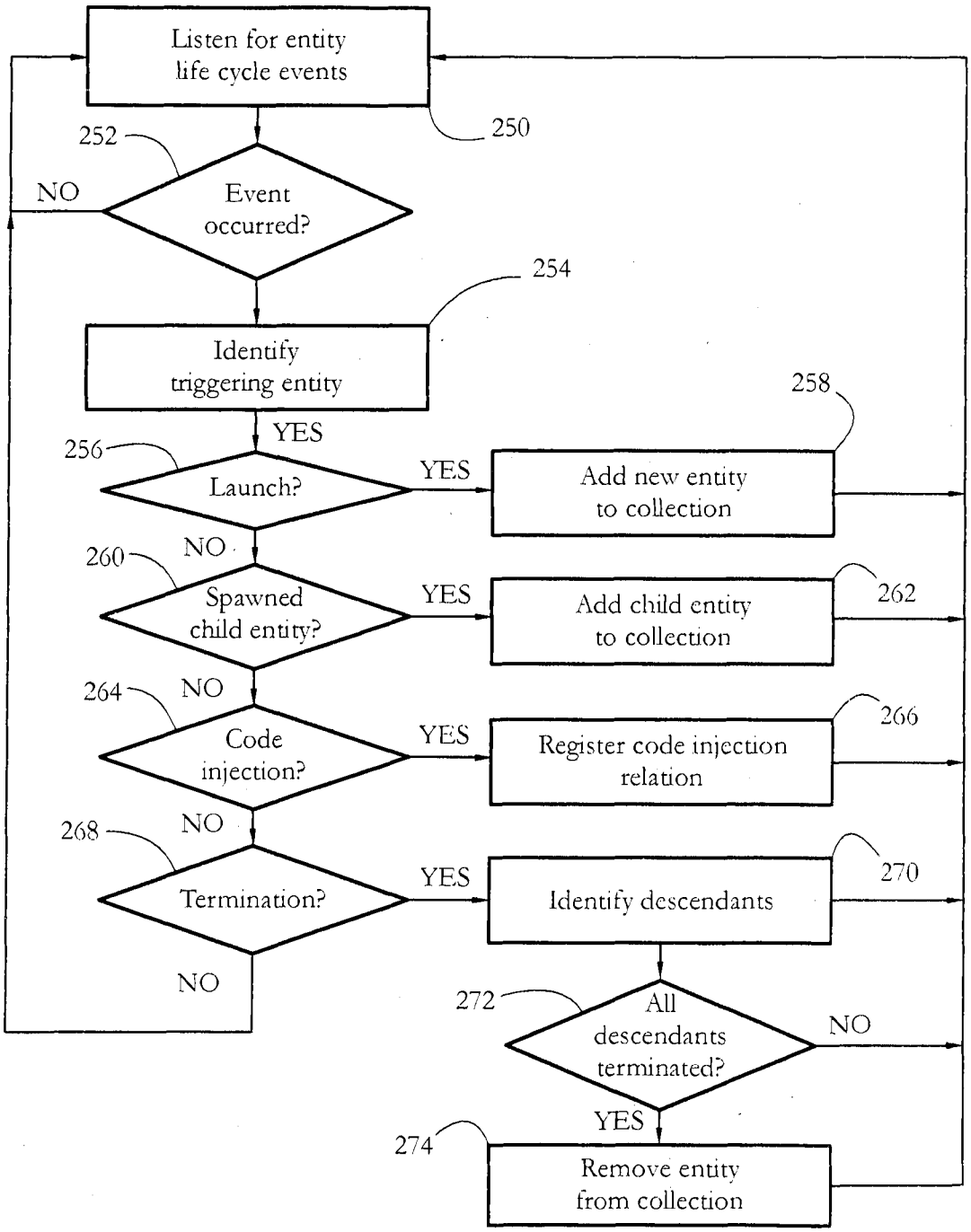
Listen for entity life cycle events
250
252
Event occurred?
NO
254
Identify triggering entity
YES
256
Launch?
YES
258
Add new entity to collection
NO
260
Spawned child entity?
YES
Add child entity to collection
262
NO
264
Code injection?
YES
Register code injection relation
266
NO
268
Termination?
YES
Identify descendants
270
NO
272
All descendants terminated?
NO
YES
274
Remove entity from collection

FIG. 4

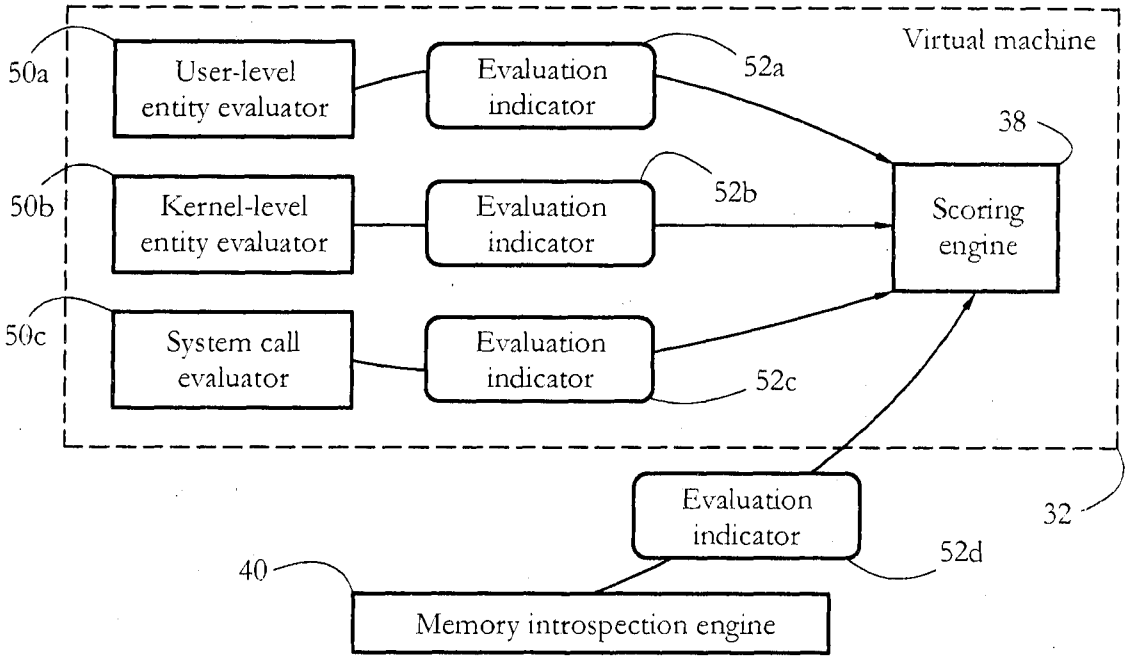
Virtual machine
50a
User-level entity evaluator
Evaluation indicator
52a
38
50b
Kernel-level entity evaluator
Evaluation indicator
52b
Scoring engine
50c
System call evaluator
Evaluation indicator
52c
Evaluation indicator
52d
32
40
Memory introspection engine

FIG. 5

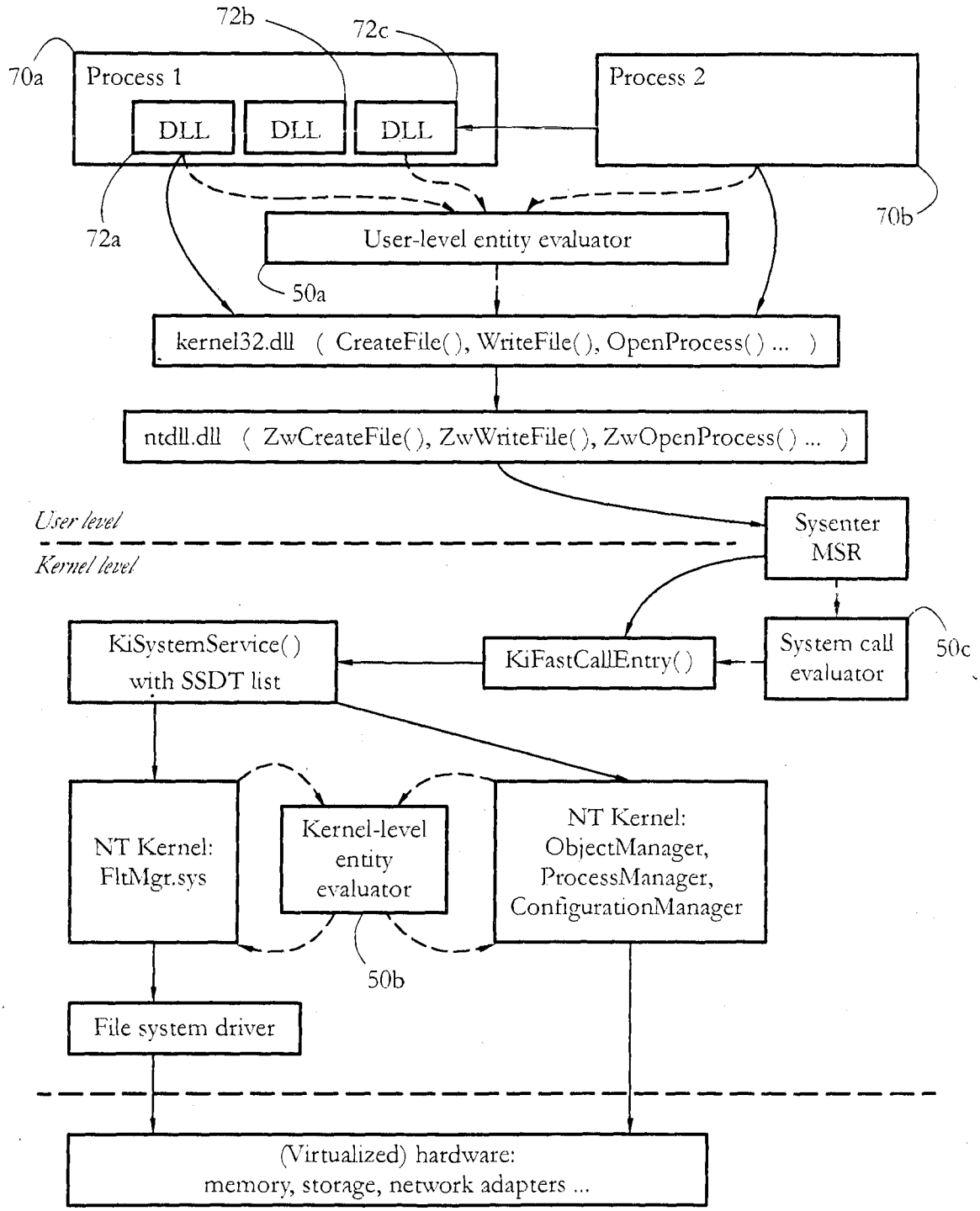
72b
72c
70a
Process 1
DLL
DLL
DLL
Process 2
70b
72a
User-level entity evaluator
50a
kernel32.dll (CreateFile( ), WriteFile( ), OpenProcess( ) ...)
ntdll.dll (ZwCreateFile( ), ZwWriteFile( ), ZwOpenProcess( ) ...)
User level
Kernel level
Sysenter
MSR
KiSystemService( )
with SSDT list
KiFastCallEntry( )
System call
evaluator
50c
NT Kernel:
FltMgr.sys
Kernel-level
entity
evaluator
NT Kernel:
ObjectManager,
ProcessManager,
ConfigurationManager
50b
File system driver
(Virtualized) hardware:
memory, storage, network adapters ...

FIG. 6

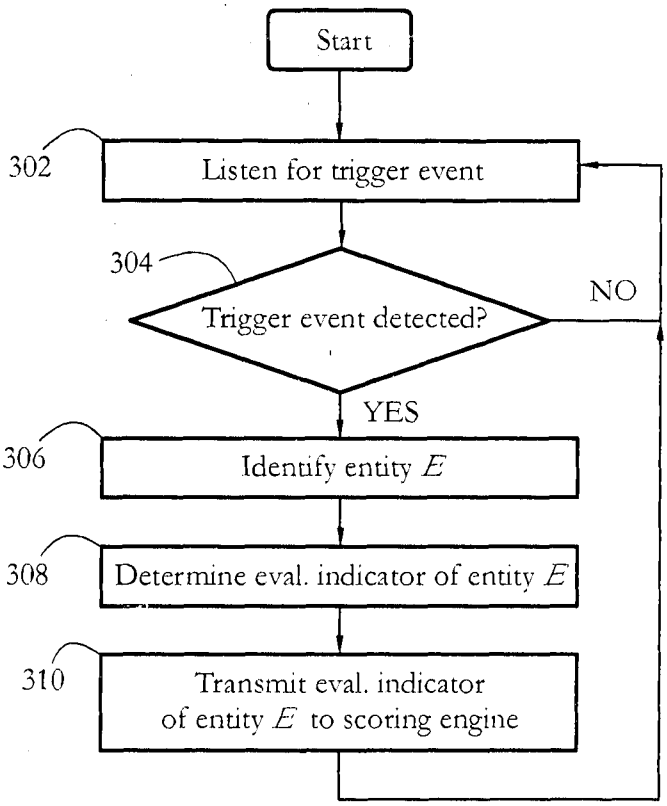
Start
302
Listen for trigger event
304
Trigger event detected?
NO
YES
306
Identify entity E
308
Determine eval. indicator of entity E
310
Transmit eval. indicator of entity E to scoring engine

FIG. 7

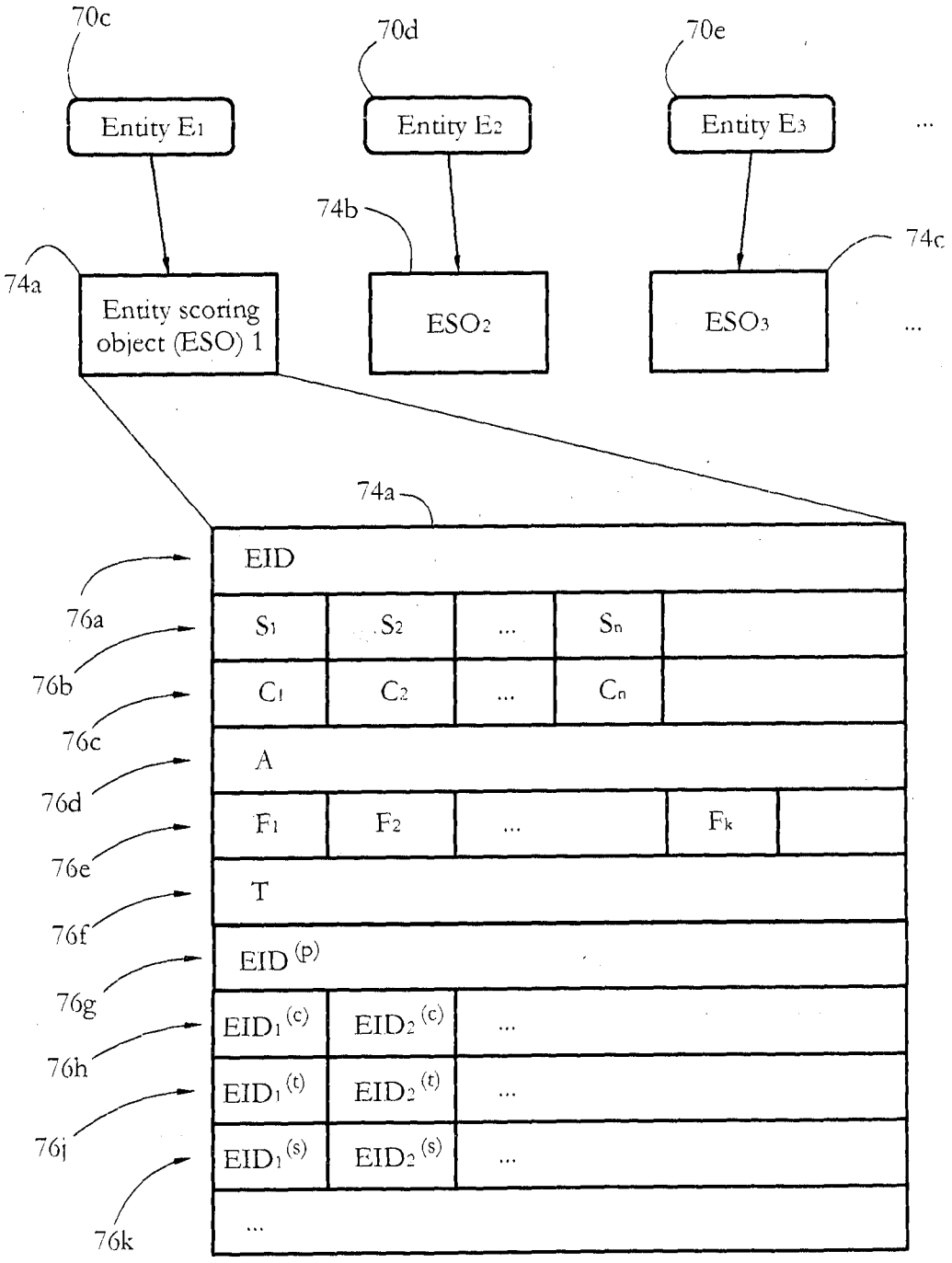
70c
70d
70e
Entity E1
Entity E2
Entity E3
...
74b
74c
74a
Entity scoring object (ESO) 1
ESO2
ESO3
...
74a
EID
76a
S1
S2
...
Sn
76b
C1
C2
...
Cn
76c
A
76d
F1
F2
...
Fk
76e
T
76f
EID (p)
76g
EID1 (c)
EID2 (c)
...
76h
EID1 (t)
EID2 (t)
...
76j
EID1 (s)
EID2 (s)
...
76k
...

FIG. 8

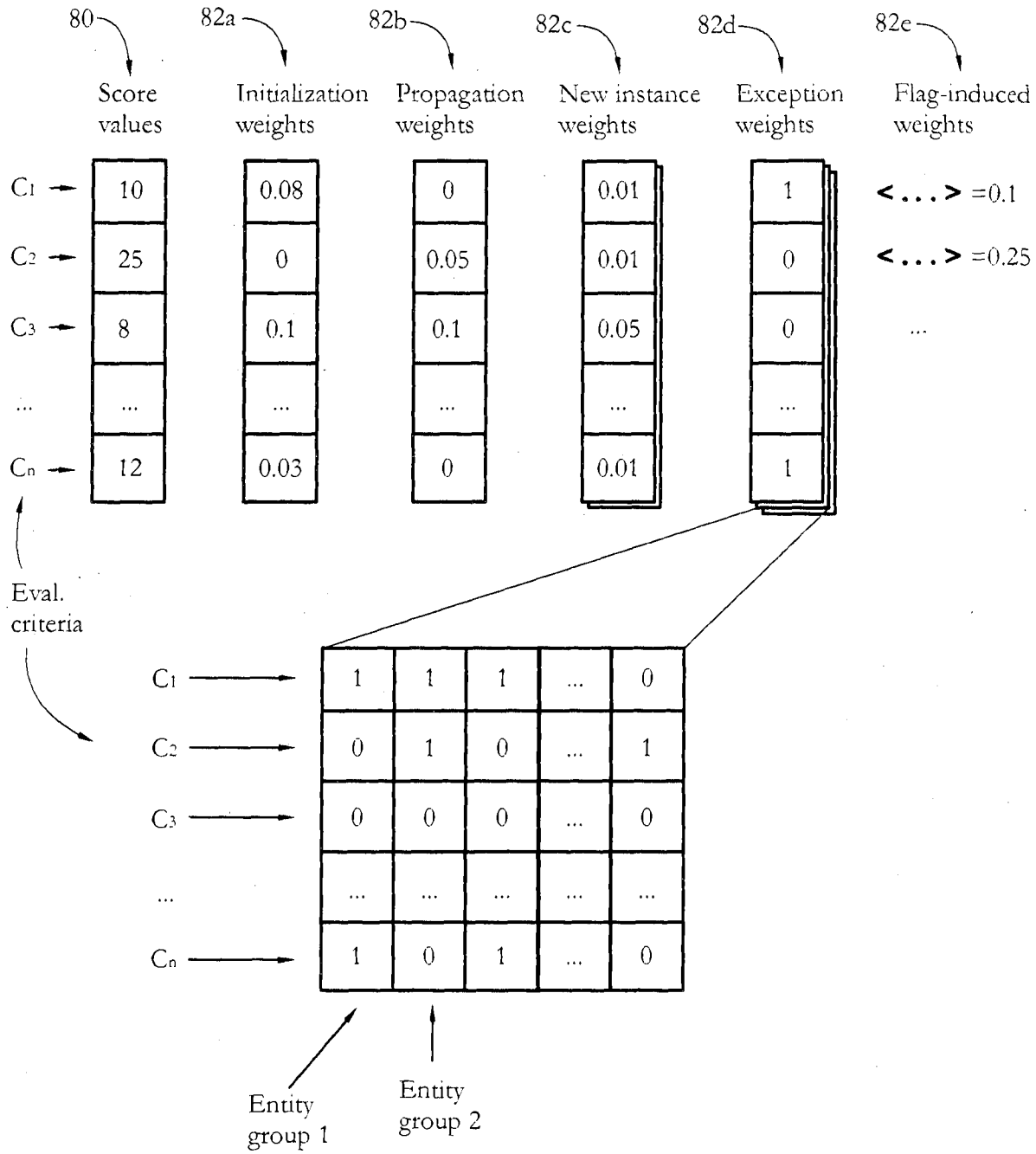
80
82a
82b
82c
82d
82e
Score values
Initialization weights
Propagation weights
New instance weights
Exception weights
Flag-induced weights
C1
C2
C3
...
Cn
10
25
8
...
12
0.08
0
0.1
...
0.03
0
0.05
0.1
...
0
0.01
0.01
0.05
...
0.01
1
0
0
...
1
<...> =0.1
<...> =0.25
...
Eval. criteria
1 1 1 ... 0
0 1 0 ... 1
0 0 0 ... 0
... ...
1 0 1 ... 0
Entity group 1
Entity group 2

FIG. 9

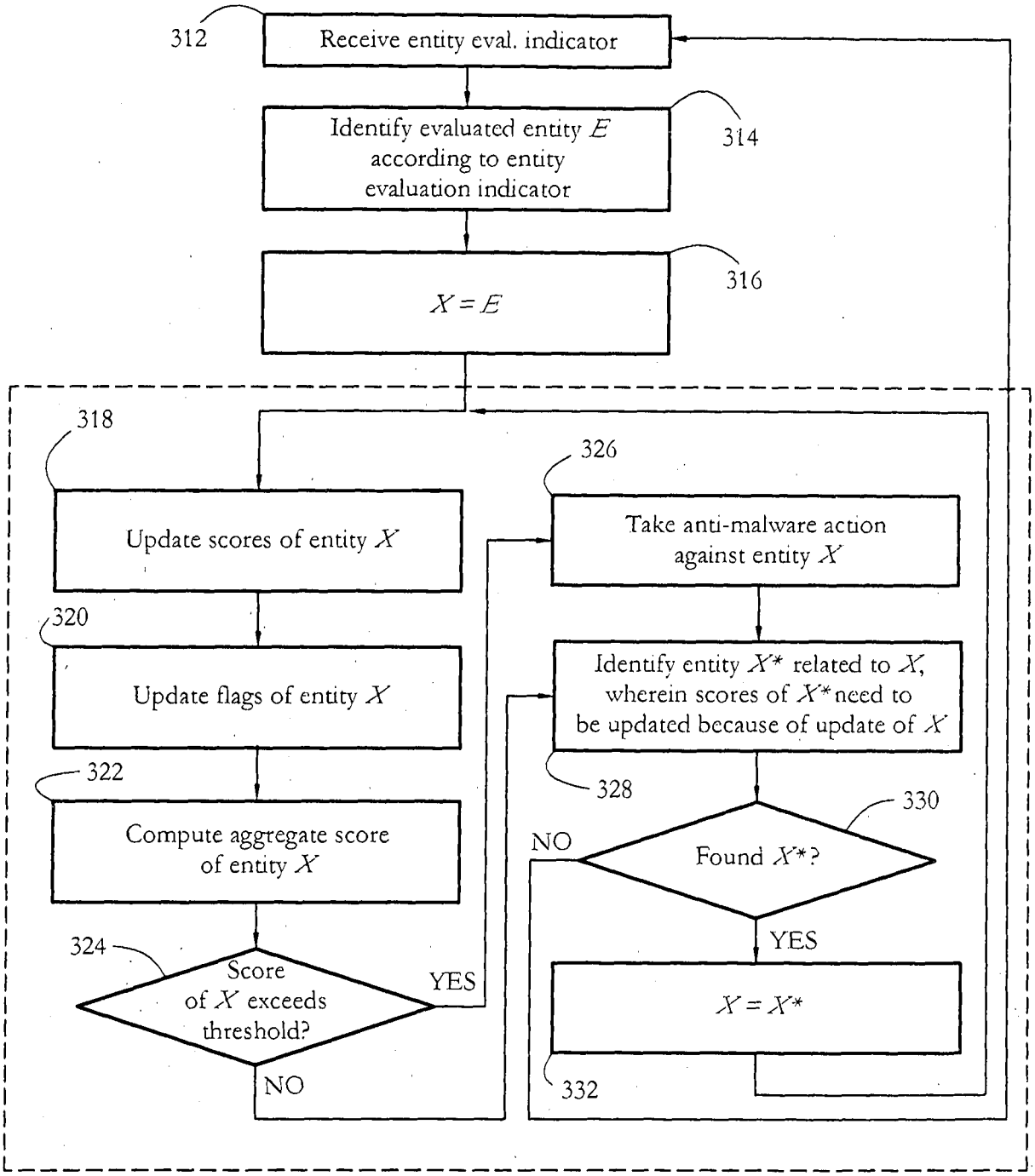
312
Receive entity eval. indicator
Identify evaluated entity E according to entity evaluation indicator
314
X = E
316
318
Update scores of entity X
320
Update flags of entity X
322
Compute aggregate score of entity X
324
Score of X exceeds threshold?
YES
NO
326
Take anti-malware action against entity X
Identify entity X* related to X, wherein scores of X* need to be updated because of update of X
328
330
Found X*?
NO
YES
X = X*
332

FIG. 10

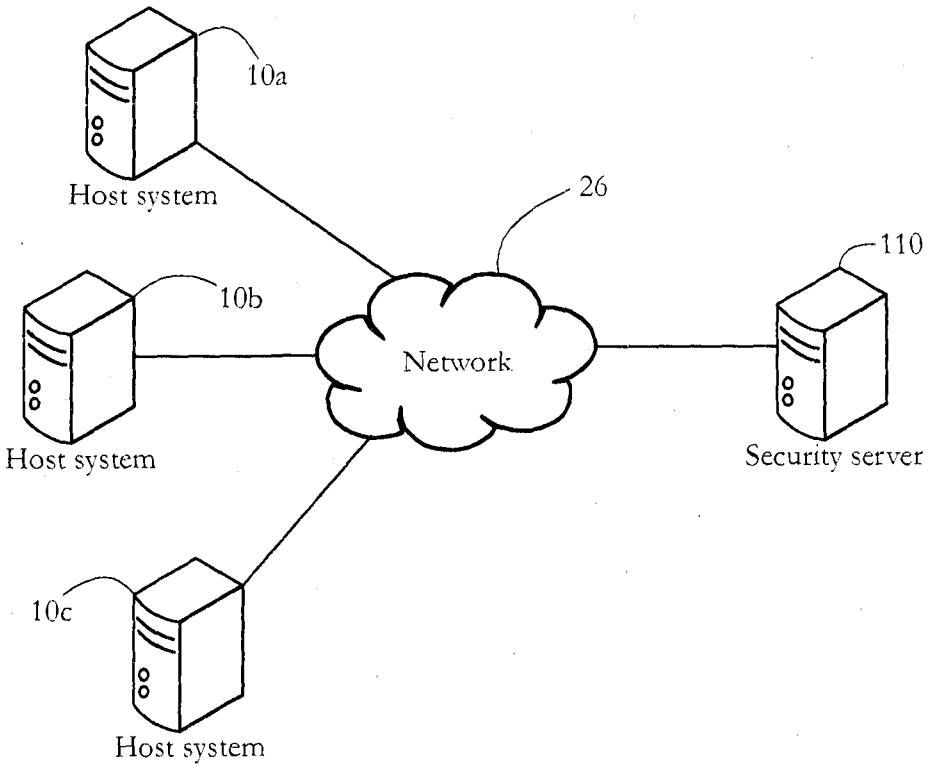
10a
Host system
26
110
10b
Network
Host system
Security server
10c
Host system

FIG. 11

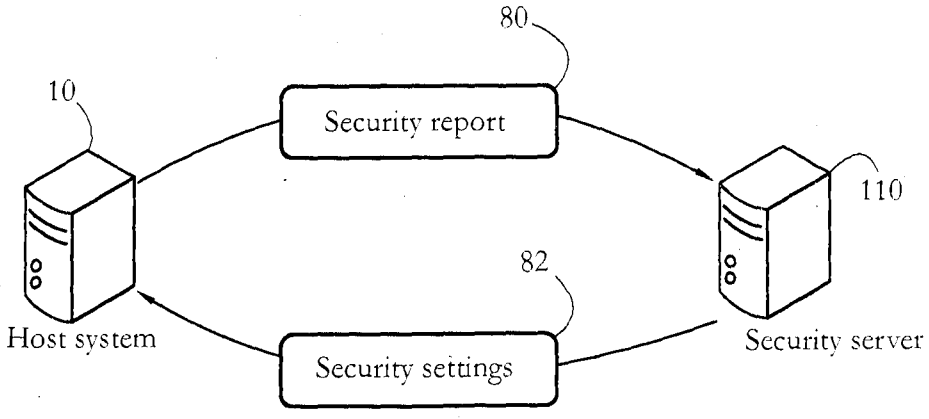
80
10
Security report
110
82
Host system
Security settings
Security server

FIG. 12