

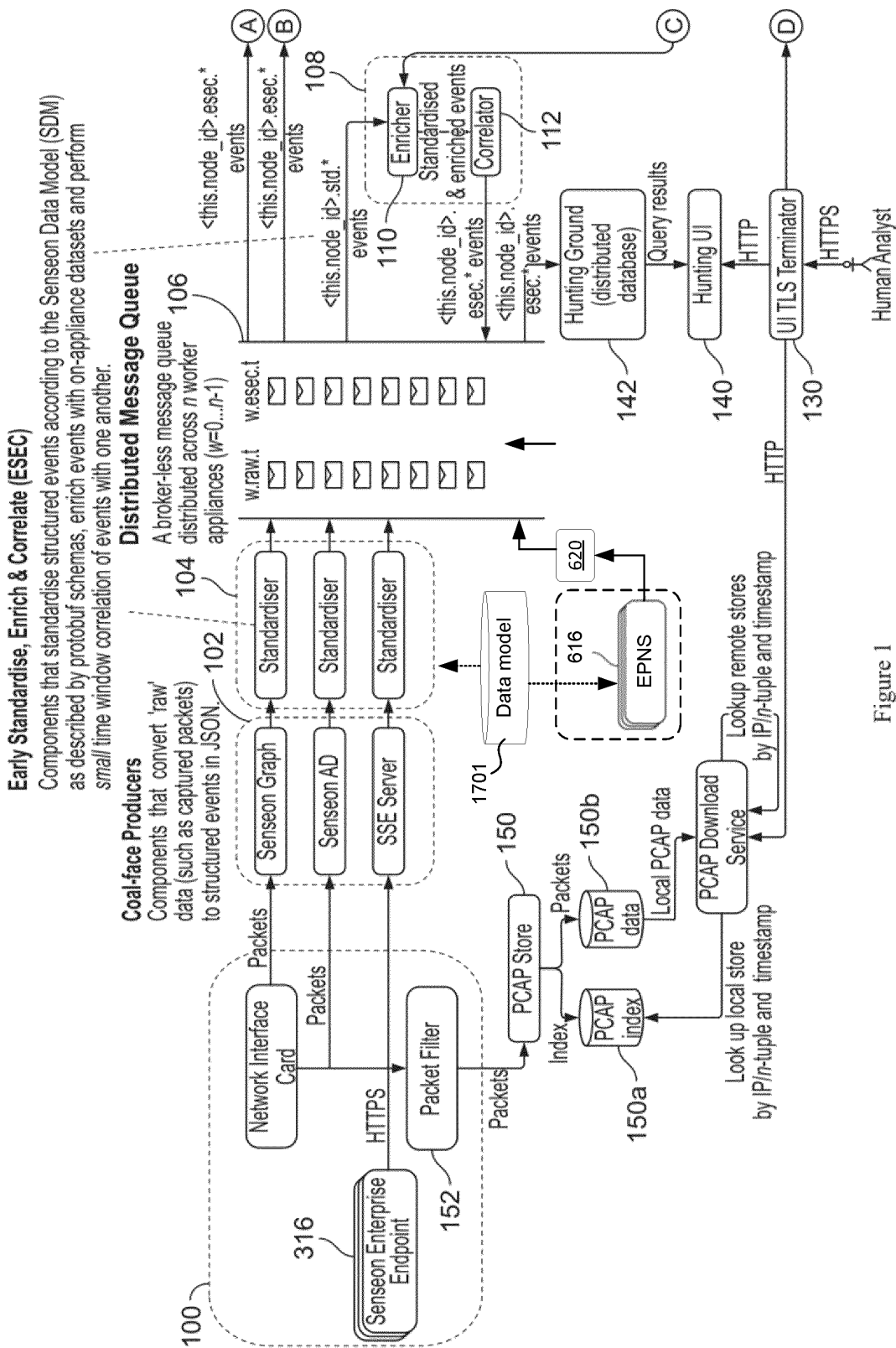


Figure 1

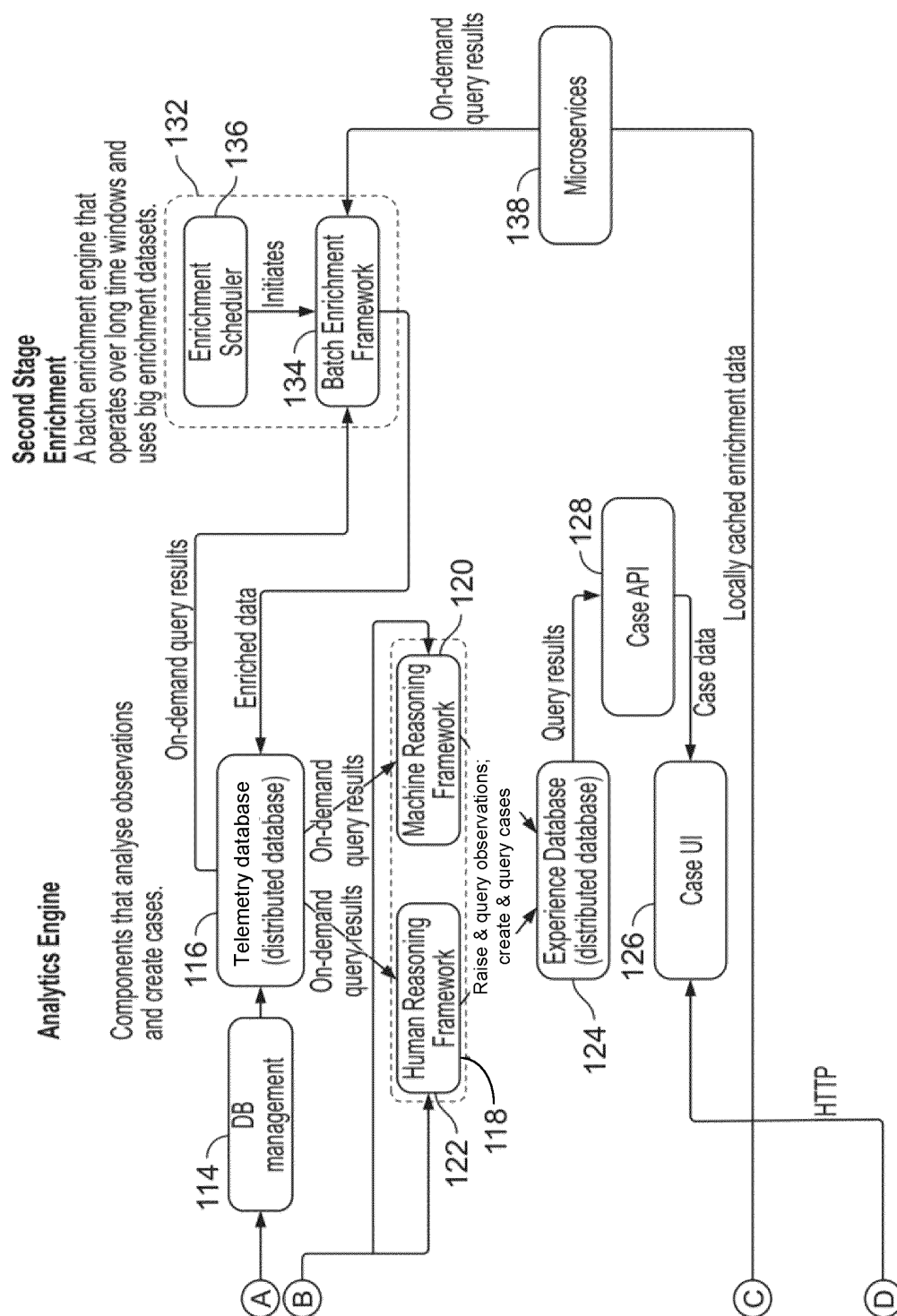


Figure 1 (continued)

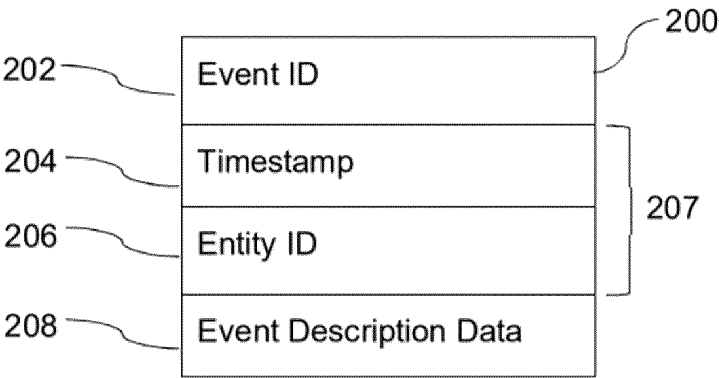


Figure 2

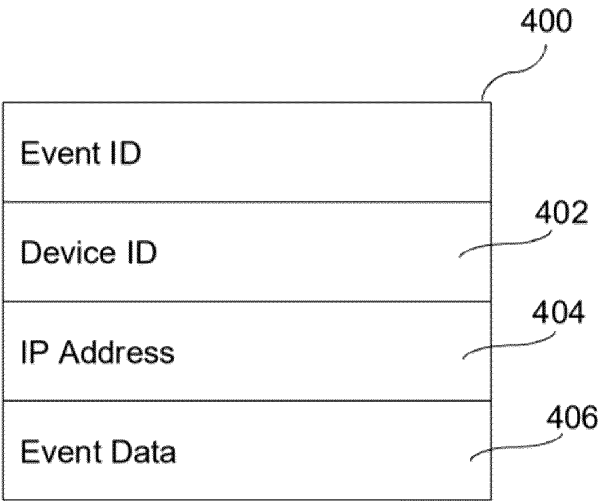


Figure 4

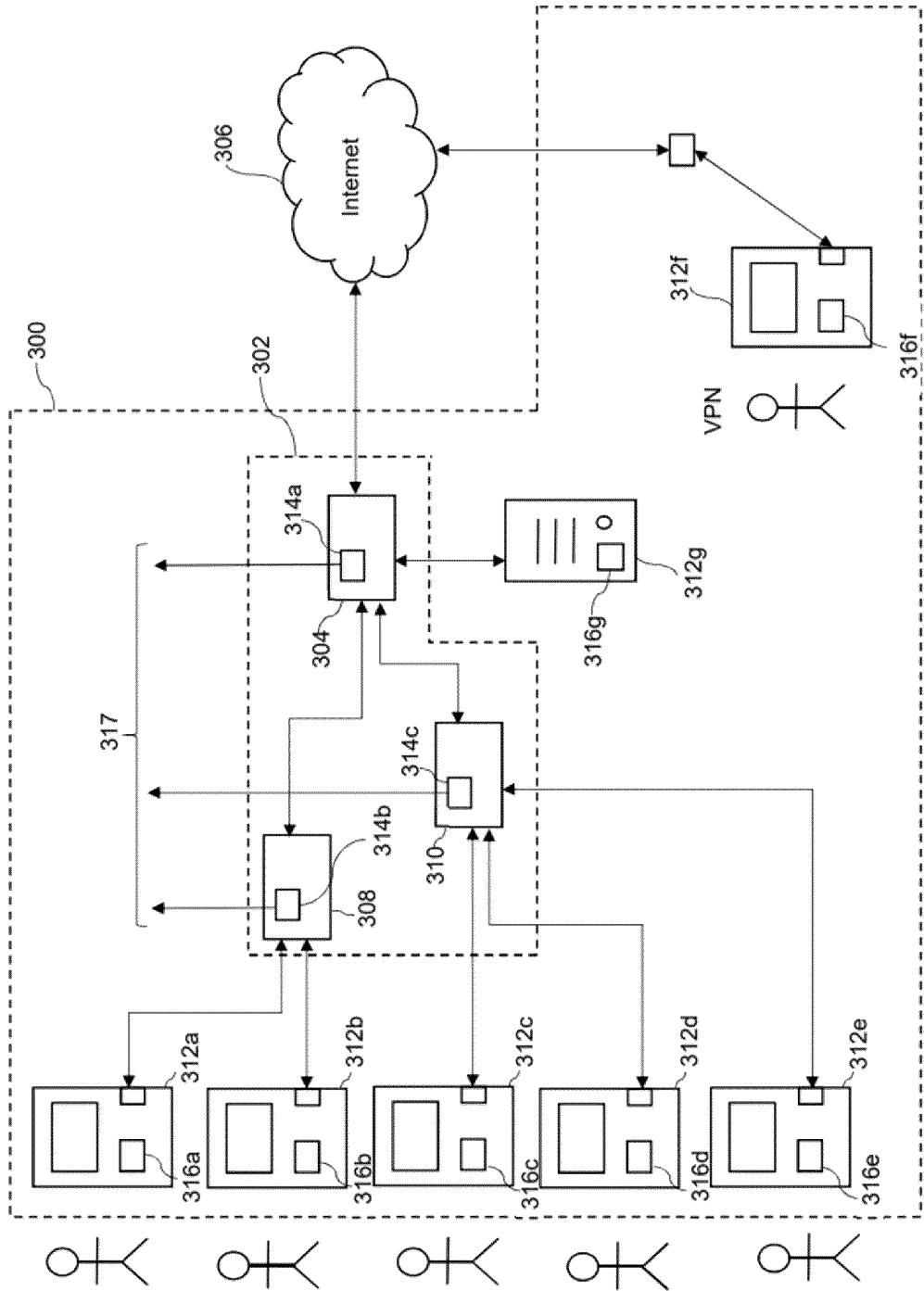
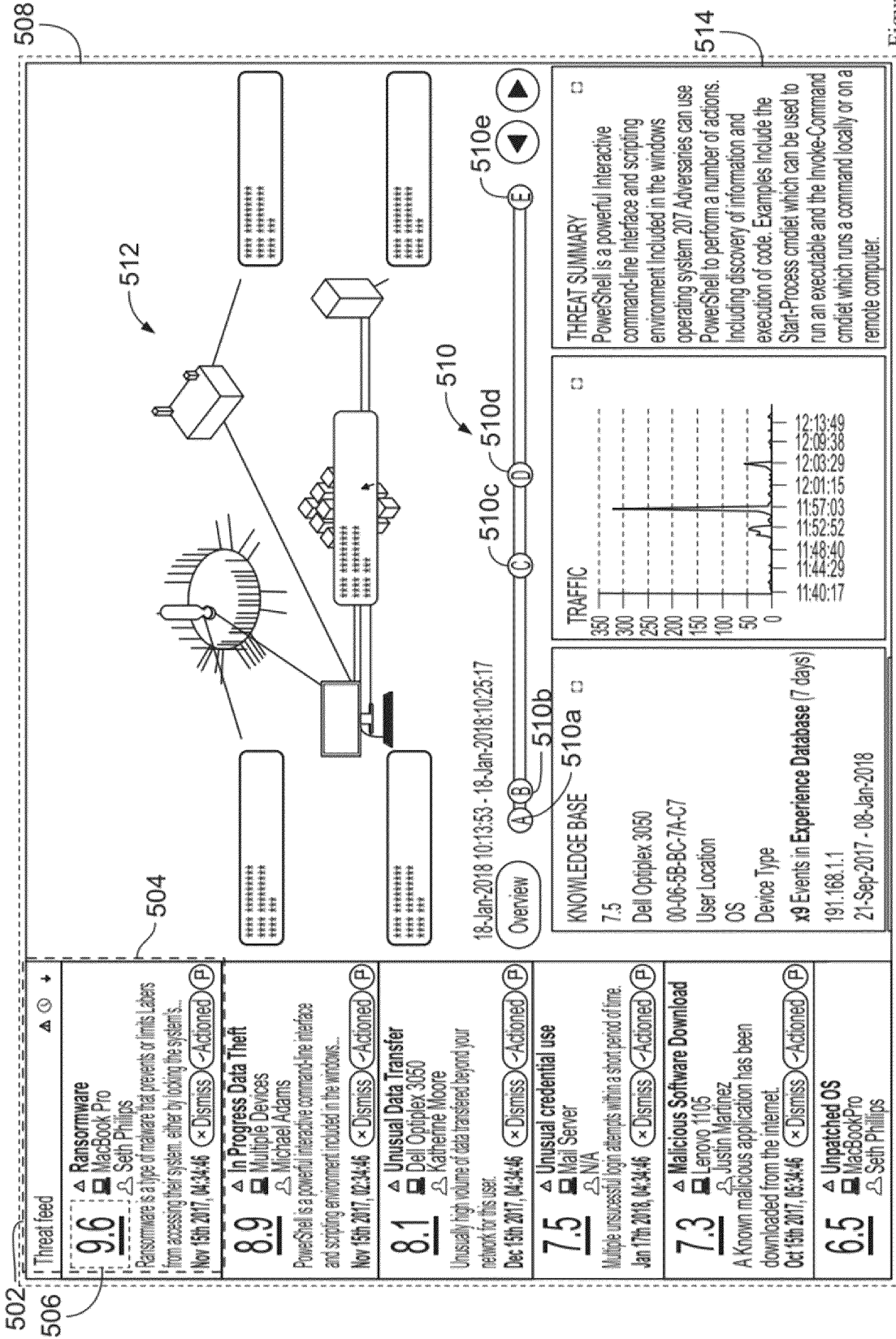
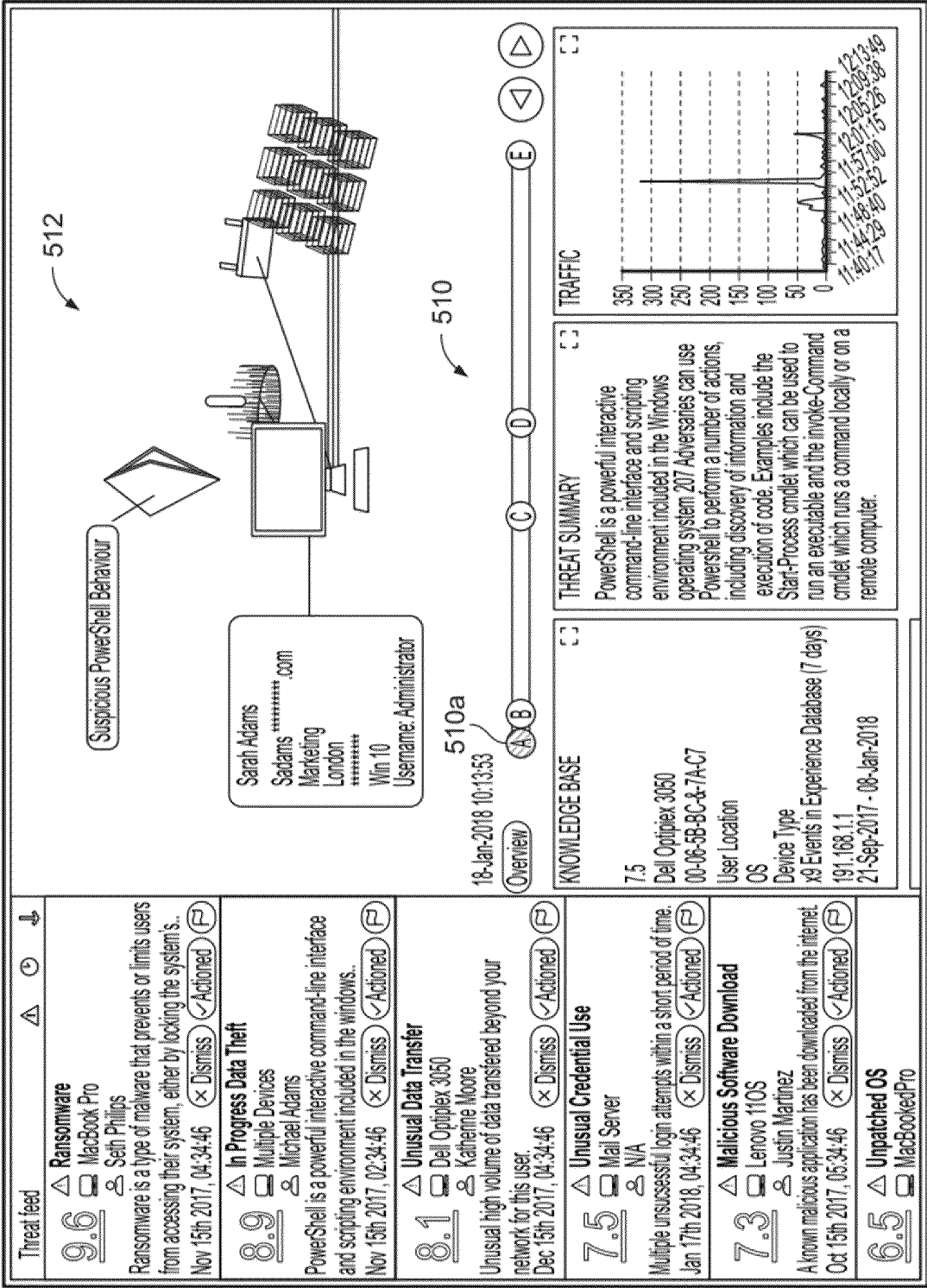


Figure 3





6.5

△ Unpatched OS

MacBook Pro

512

Suspicious PowerShell Behaviour

Sarah Adams

Sadams *****.com

Marketing London *****

Win 10

Username: Administrator

510

510a

18-Jan-2018 10:13:53

Overview

A

B

C

D

E

THREAT SUMMARY

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system 207 Adversaries can use Powershell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the invoke-Command cmdlet which runs a command locally or on a remote computer.

TRAFFIC

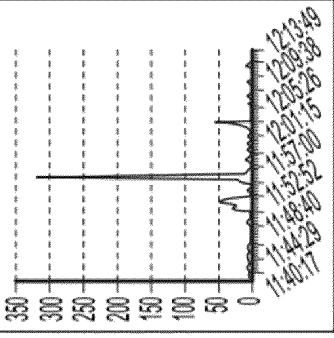
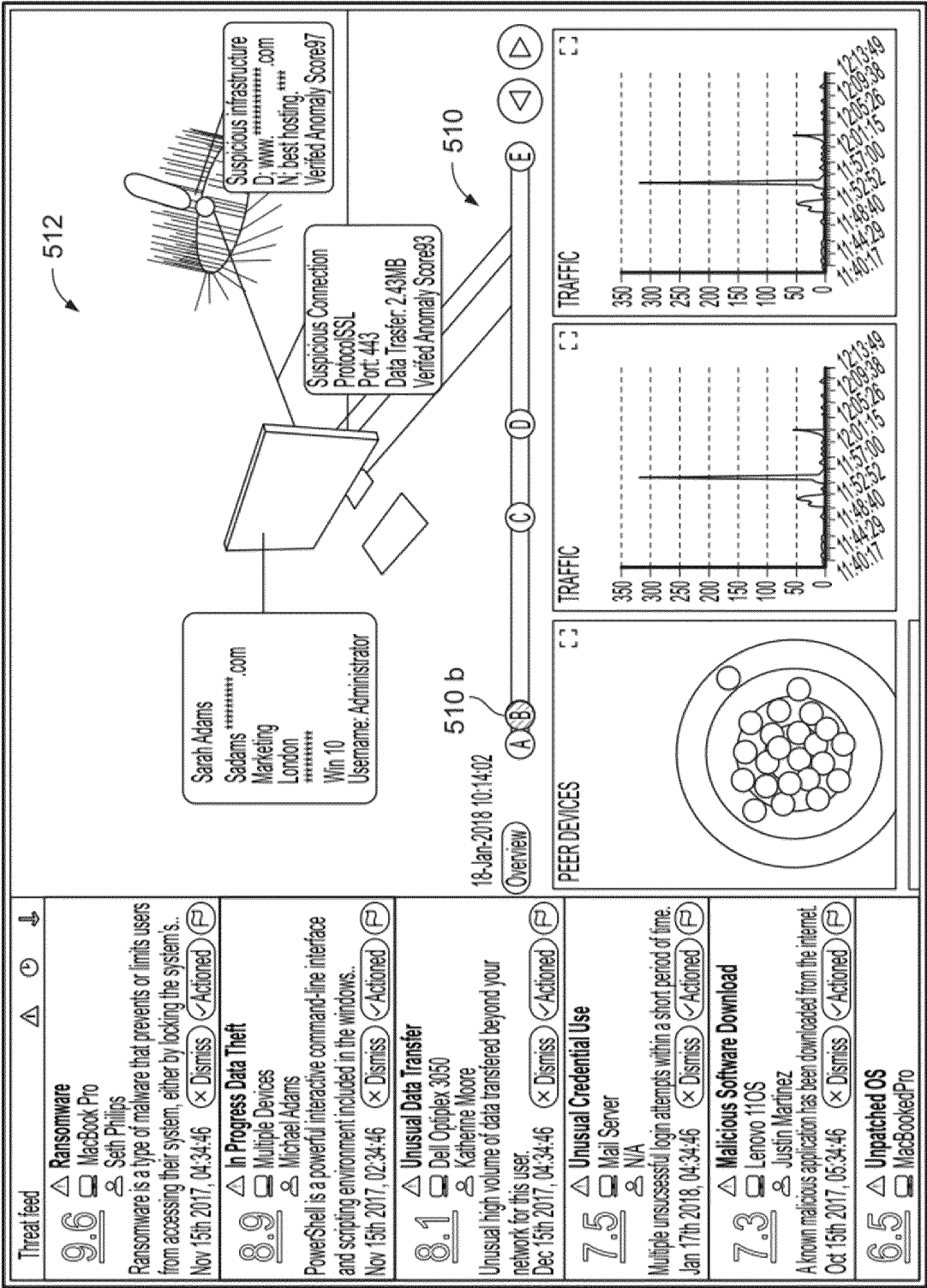


Figure 5A



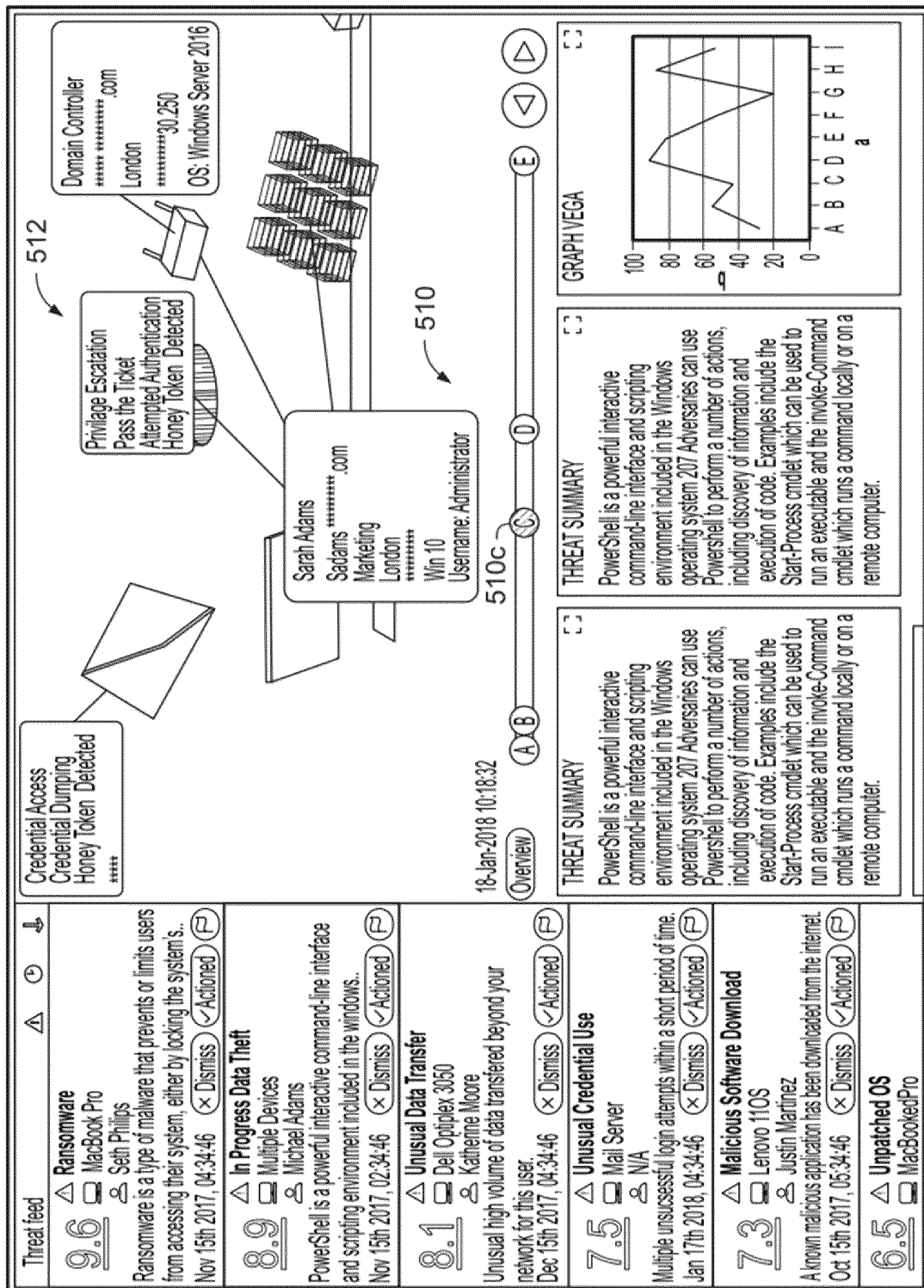


Figure 5C

9/17

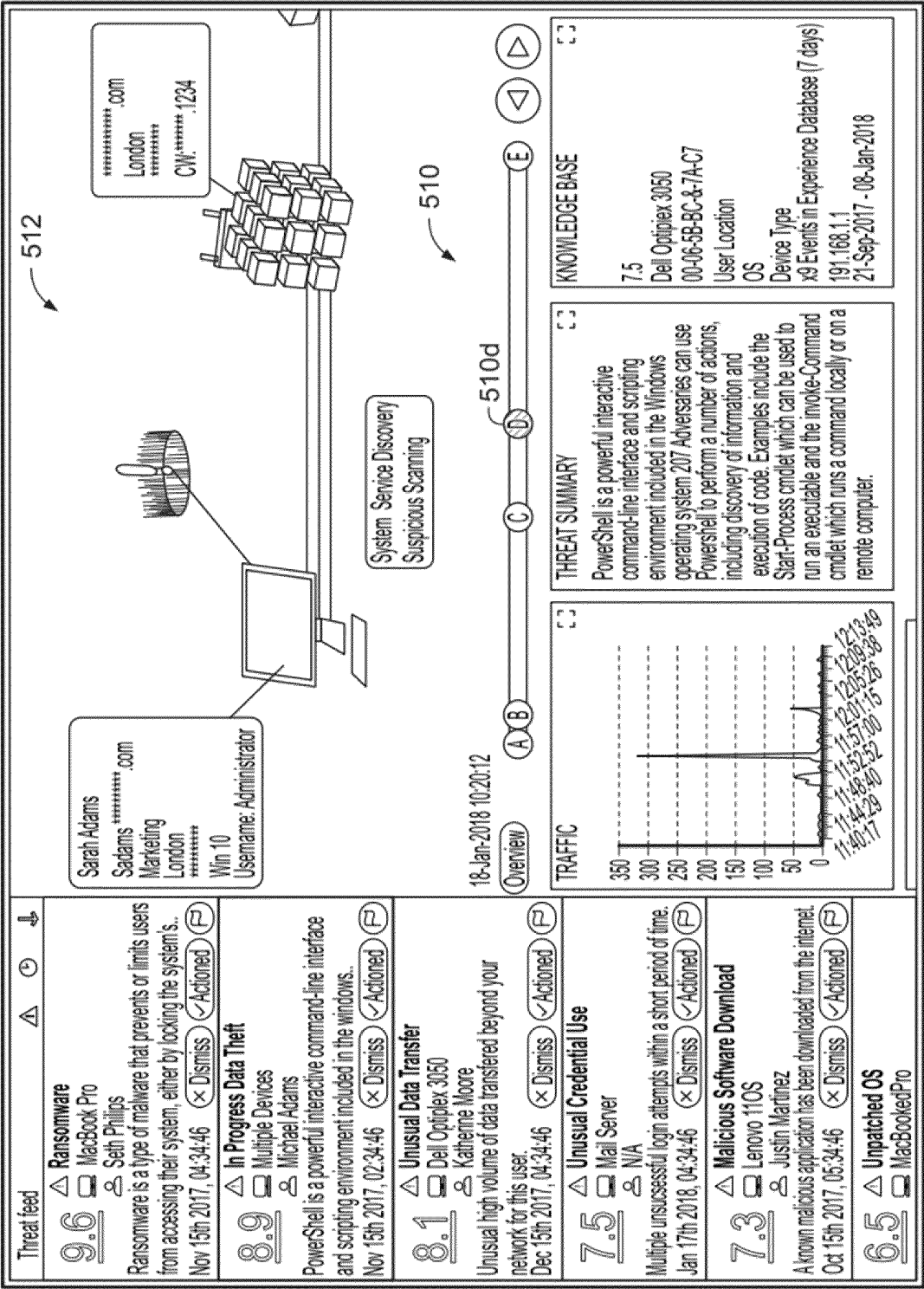
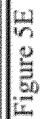


Figure 5D



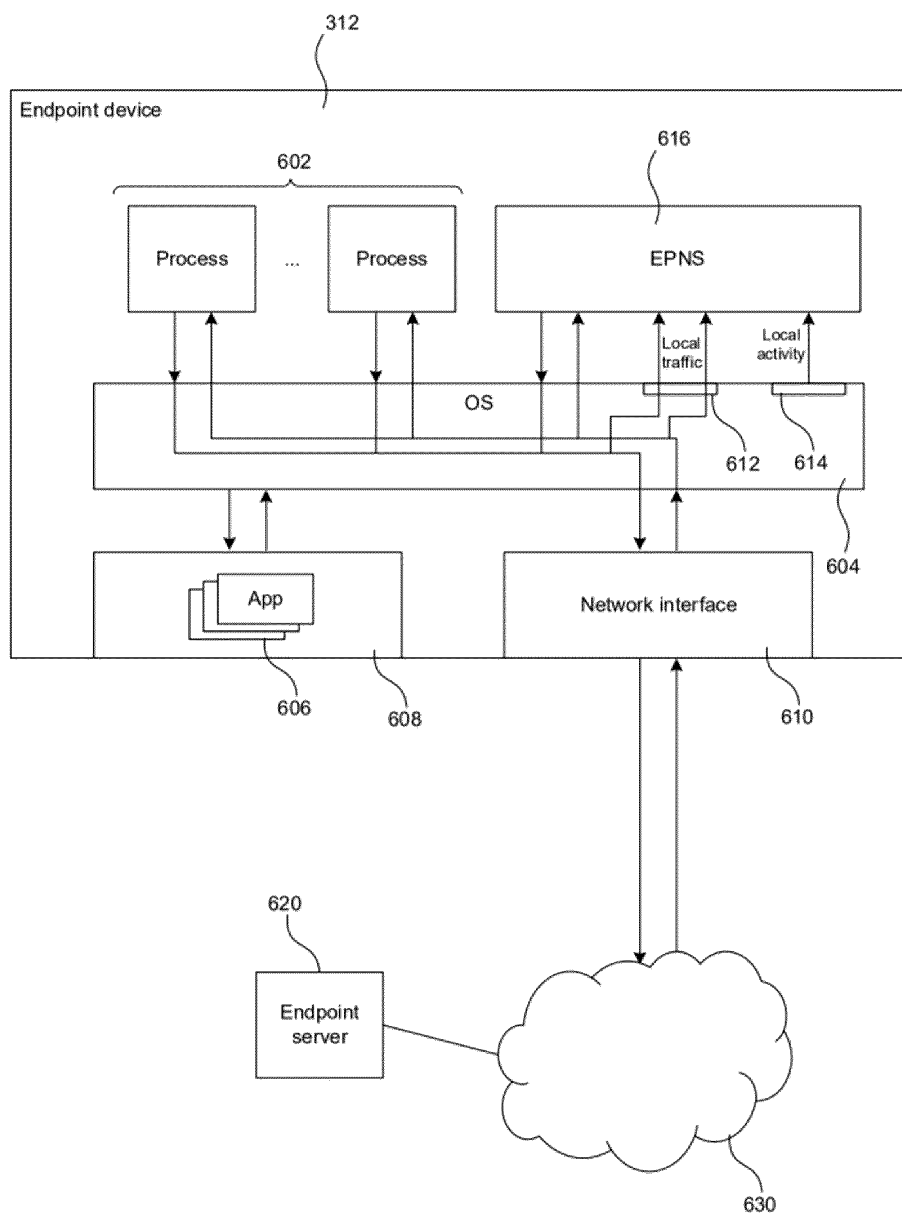


Figure 6

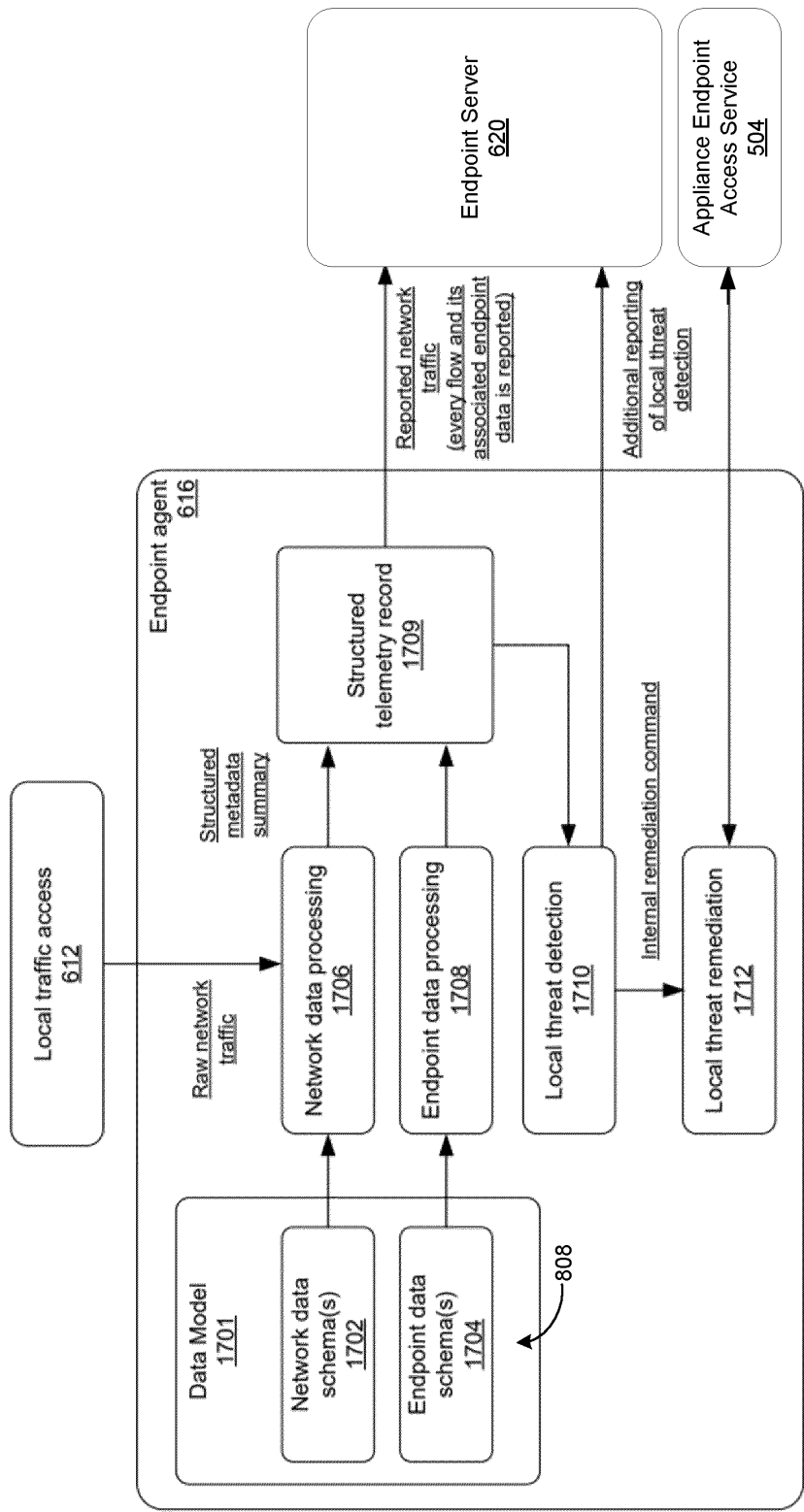


Figure 7

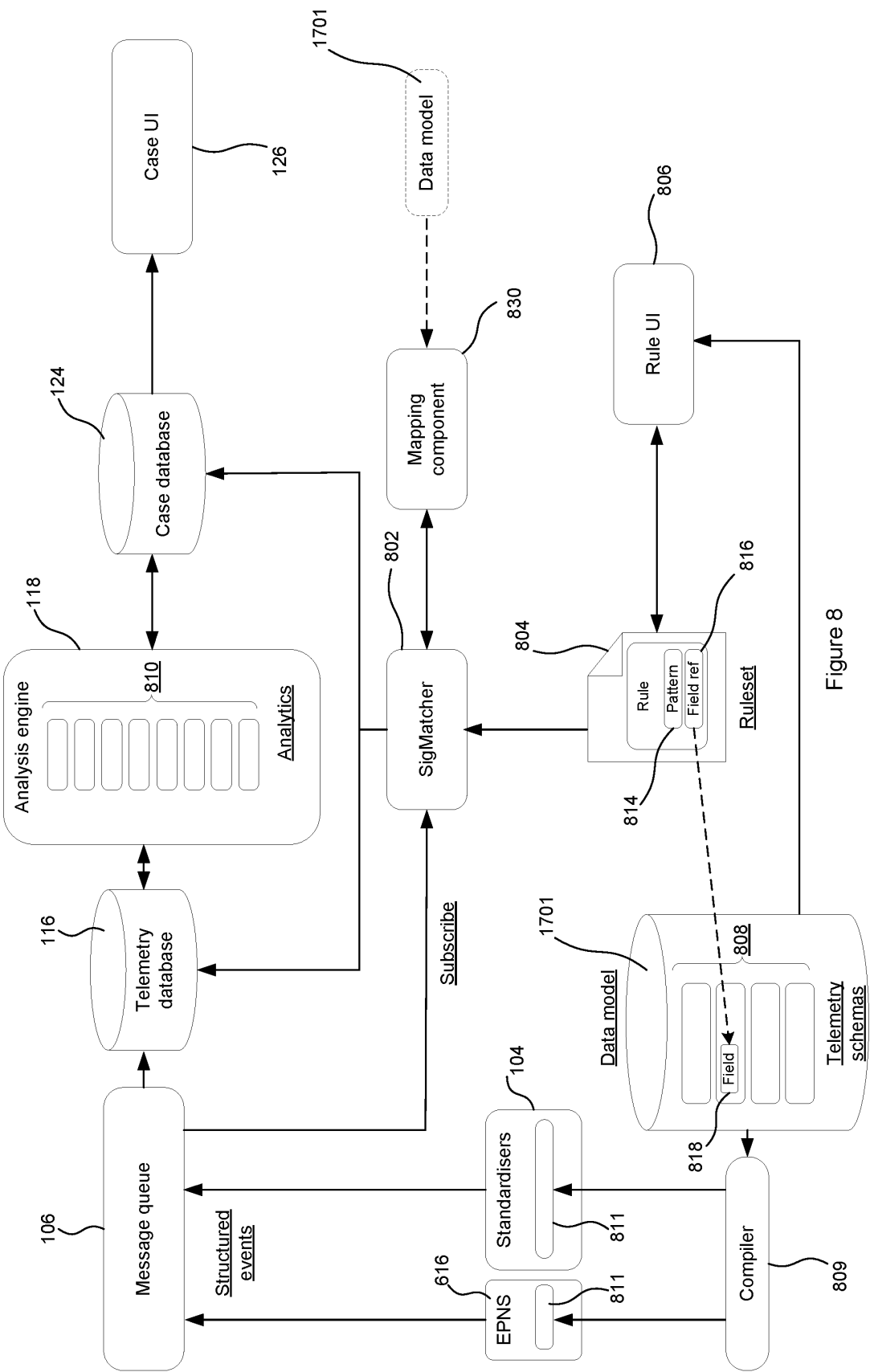


Figure 8

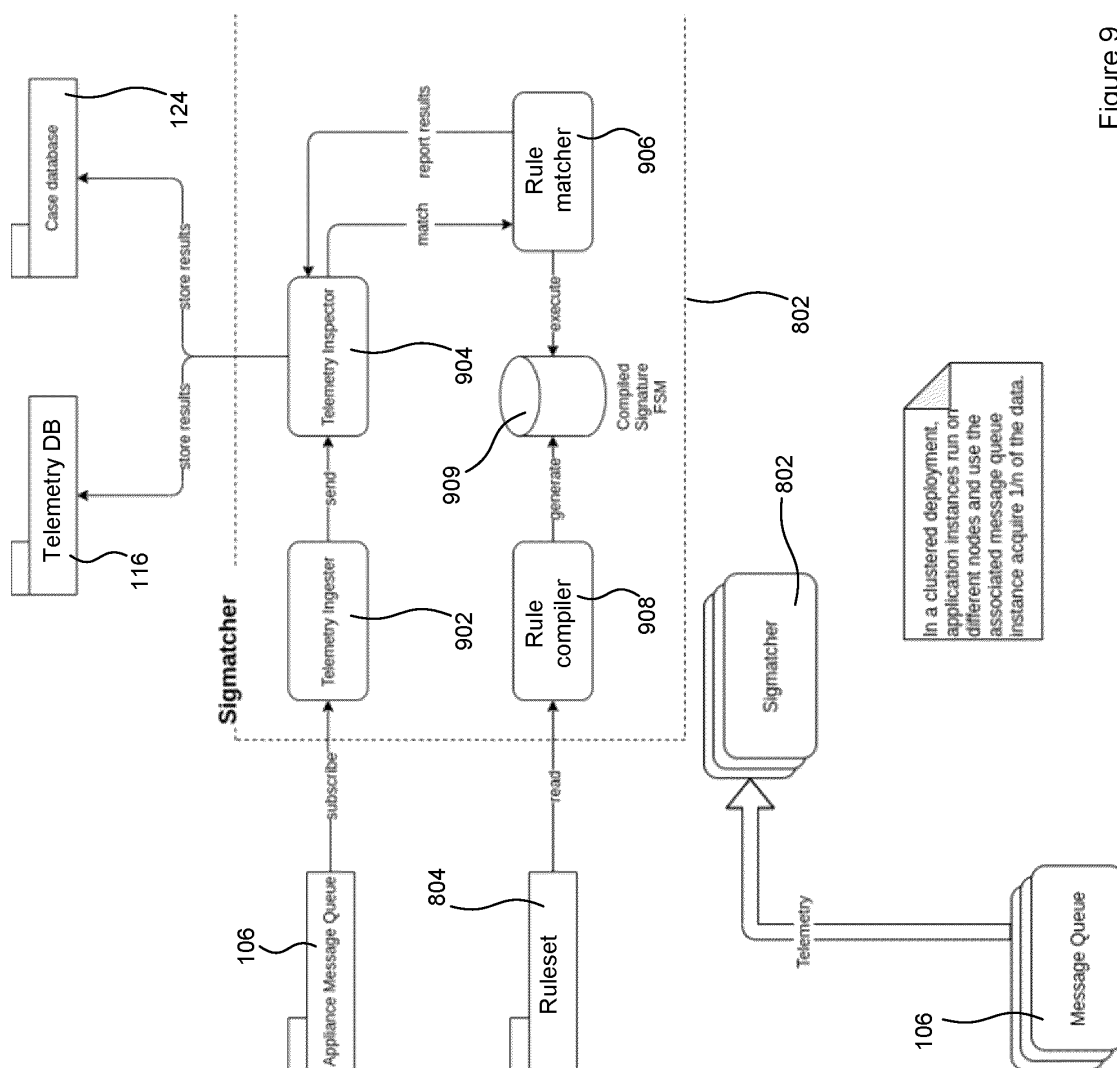


Figure 9

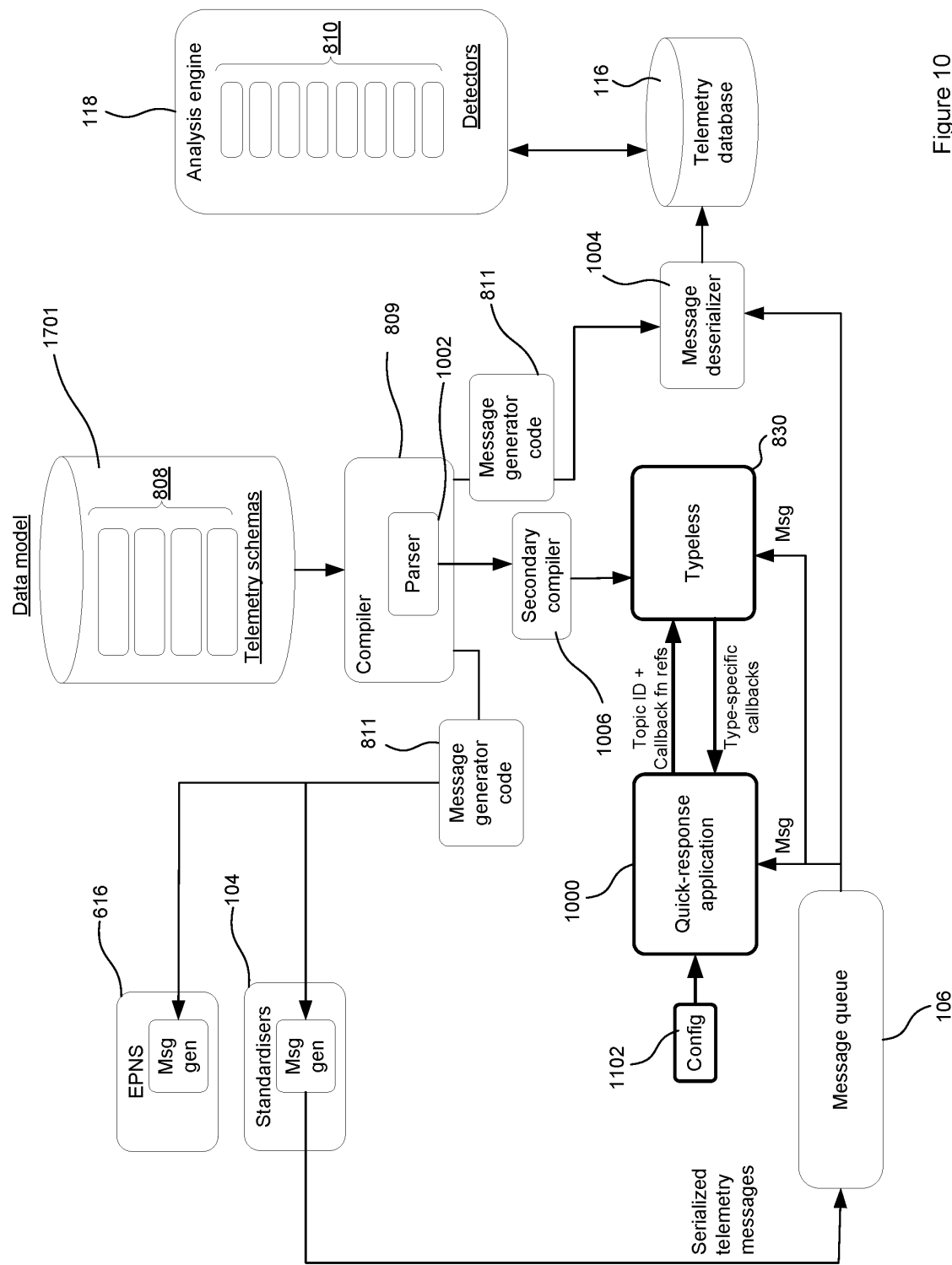


Figure 10

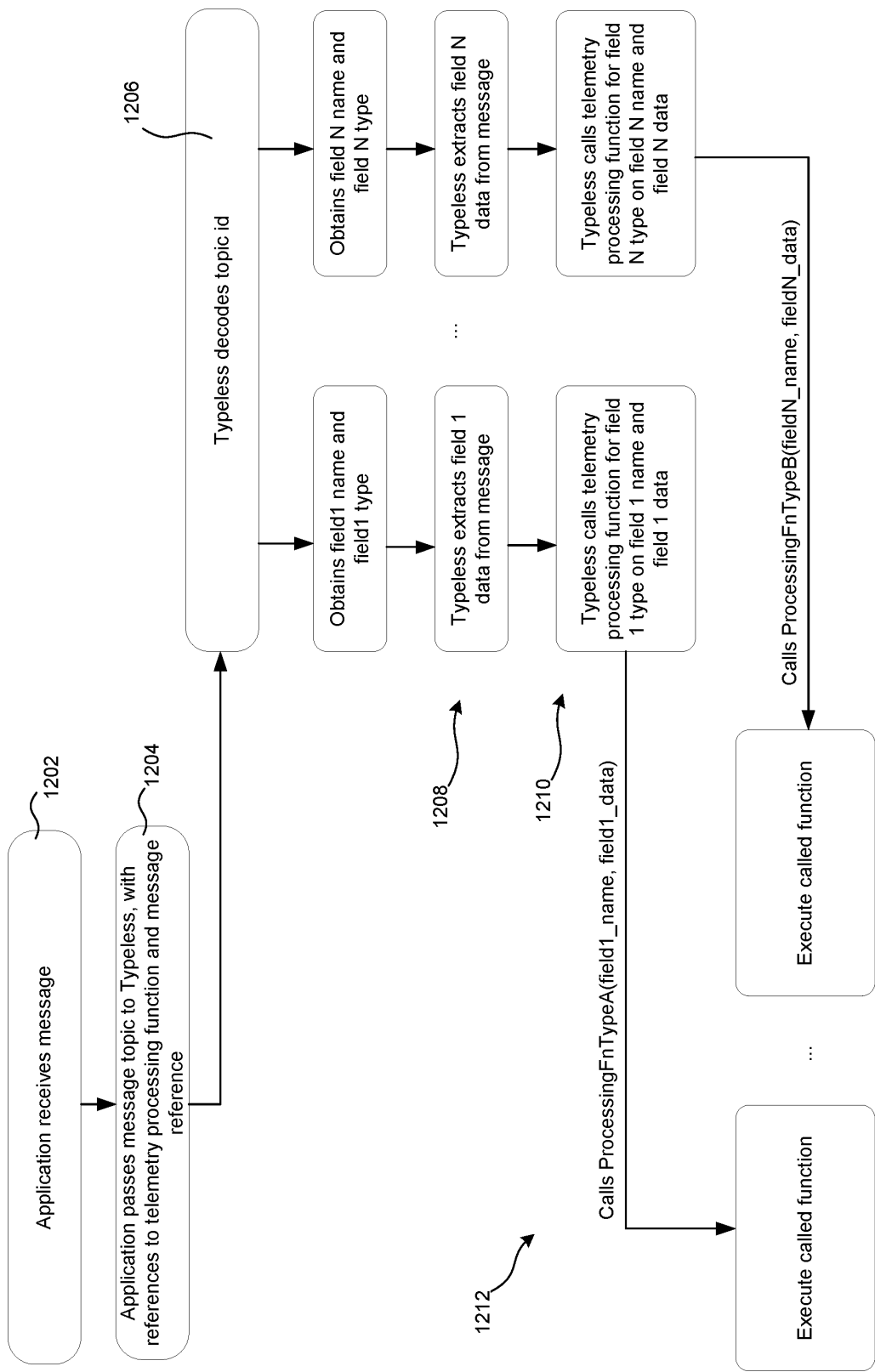


Figure 12