

CLAIMS

1. A computer system comprising:
 - a data repository storing global policy data that describes policies;
 - a plurality of computer assets, implemented at least partially by first computer hardware, each asset of the plurality of computer assets configured to: receive messages from client devices; store local policy data describing the policies at a computing device that implements the assets, wherein the policies stored in a global resource cache determine rules for Uniform Resource Identifier (URIs), the policies stored in a subject rules cache determine rules for subjects, and the policies stored in a subject resource cache determine rules for subjects requesting URIs; determine which of the policies apply to which of the messages by determining whether to exclude the messages from policy enforcement, determining whether messages identify URIs stored in the global resource cache, determining whether a customer ID of the messages is stored in the subject rules cache or the subject resource cache, determining whether a source IP address of the messages is stored in the subject rules cache or the subject resource cache, and determining whether a device identifier of the message is stored in the subject rules cache or the subject resource cache; identify policy-based actions to perform with respect to the messages based on which of the policies apply to which of the messages; send message information logged from the messages to an analyzer component; and update the local policy data to reflect updates to the global policy data;
 - wherein the messages indicated designated actions for the plurality of assets to perform and wherein each asset is configured to perform the applicable policy-based actions instead of or in addition to the indicated designated actions for messages to which the policies apply; and
 - an analyzer component, implemented at least partially by second computer hardware, configured to: receive the message information from each of the plurality of computer assets; collectively analyze the message information from each of the plurality of computer assets; generate new policies based on collectively analyzing the message information; and update the global policy data to describe the new policies.

2. The computer system of claim 1, wherein each asset of the plurality of computer assets is deployed at an edge of a first network, and wherein the client devices are deployed with a second network.

3. The computer system of Claim 1, wherein the plurality of computer assets and the analyzer are deployed in a first region of the computer system, the computer system further comprising one or more additional regions, each region comprising a separate plurality of computer assets and a separate analyzer, the data repository being shared between the first region and the one or more additional regions.

4. The computer system of Claim 1, wherein each policy of the policies is a data structure that indicates logic for determining whether the policy applies to a given message, as well as one or more instructions indicating one or more particular policy-based actions to perform with respect to the given message if the policy applies to the given message.

5. The computer system of Claim 1, wherein the analyzer is further configured to: identify one or more of the new policies based on determining, from the collectively analyzed message information, that a condition described by a system-level policy exists; generate one or more asset-level policies comprising logic for identifying messages to block or redirect in view of the described condition; and update the global policy data to include the generated one or more asset-level policies.

6. The computer system of Claim 1, wherein the analyzer is further configured to: identify a distributed attack on the computer system based on the collectively analyzed message information; generate a first policy comprising logic for identifying messages involved in the distributed attack; and update the global policy data to describe the first policy.

7. The computer system of Claim 1,
wherein the analyzer is further configured to, based on the collectively analyzed message information: identify an attack that is occurring at a first asset of the plurality of computer assets; generate a first policy comprising logic for identifying messages involved in the attack; and update the global policy data to describe the first policy;
wherein a second asset of the plurality of computer assets is configured to: based on the updated global policy data, update the local policy data of the second asset to describe the first policy, the second asset having not yet received

messages involved in the attack at a time the local policy data of the second asset is updated; and, based on the first policy, block or redirect a message involved in the attack.

8. The computer system of Claim 1, wherein a policy-based action indicated by a given policy of the policies is one of: blocking any message to which the given policy applies, redirecting any message to which the given policy applies, or allowing an asset to respond normally to any message to which the given policy applies.

9. The computer system of Claim 1, wherein an asset of the plurality of computer assets is configured to apply policies, from the local policy data of the asset, to messages, even when the analyzer component and the data repository are inaccessible to the asset.

10. A data processing method comprising:
storing, at a computer asset, local policy data describing policies, wherein the policies stored in a global resource cache determine rules for Uniform Resource Identifier (URIs), the policies stored in a subject rules cache determine rules for subjects, and the policies stored in a subject resource cache determine rules for subjects requesting URIs;
receiving, at the computer asset, messages from client devices;
wherein the messages indicate designated actions for the plurality of assets to perform,
wherein each asset is configured to perform the applicable policy-based actions instead of or in addition to the indicated designated actions for messages to which the policies apply;
determining, at the computer asset, which of the policies apply to which of the messages, by determining whether to exclude the messages from policy enforcement, determining whether the messages identify URIs stored in the global resource cache, determining whether a customer ID of the messages is stored in the subject rules cache or the subject resource cache, determining whether a source IP address of the messages is stored in the subject rules cache or the subject resource, and determining whether a device identifier of the message is stored in the subject rules cache or the subject resource cache;
identifying, at the computer asset, policy-based actions to perform with respect to the messages based on which of the policies apply to which of the messages;

sending, from the computer asset, message information logged from the messages to an analyzer component; and
updating, by the computer asset, the local policy data to reflect updates to global policy data generated by the analyzer component;
wherein the computer asset is implemented by one or more computing devices.

11. The method of Claim 10, wherein each policy of the policies is a data structure that indicates logic for determining whether the policy applies to a given message, as well as one or more instructions indicating one or more particular policy-based actions to perform with respect to the given message if the policy applies.

12. The method of Claim 10,
wherein the messages indicate designated actions for the plurality of computer assets to perform;
the method further comprising performing applicable policy-based actions instead of or in addition to the designated actions indicated for messages to which the policies apply.

13. The method of Claim 10, further comprising applying policies from the local policy data to messages even when the analyzer component and the global policy data are inaccessible to the asset.

14. The method of Claim 10, further comprising:
receiving, at the analyzer component, message information logged at each asset of a plurality of computer assets, including the computer asset;
collectively analyzing, by the analyzer component, the message information logged at each of the plurality of computer assets;
generating, by the analyzer component, new policies based on collectively analyzing the message information;
updating, by the analyzer component, the global policy data to describe the new policies.

15. A data processing method comprising:
receiving message information from each asset of a plurality of computer assets, the message information describing messages received by the asset;
wherein the messages indicate designated actions for the plurality of assets to perform, wherein each asset is configured to perform the applicable policy-

based actions instead of or in addition to the indicated designated actions for messages to which the policies apply;
collectively analyzing the message information from each of the plurality of computer assets;
generating policies based on collectively analyzing the message information, wherein the policies stored in a global resource cache determine rules for Uniform Resource Identifiers (URIs), the policies stored in a subject rules cache determine rules for subjects, and the policies stored in a subject resource cache determine rules for subjects requesting URIs, the policies describing logic for identifying messages to which the policies apply, including determining whether to exclude the messages from policy enforcement, determining whether the messages identify URIs stored in the global resource cache, determining whether a customer ID of the messages is stored in the subject rules cache or the subject resource cache, determining whether a source IP address of the messages is stored in the subject rules cache or the subject resource cache, and determining whether a device identifier of the message is stored in the subject rules cache or the subject resource cache, as well as policy-based actions to perform with respect to the messages to which the policies apply;
updating a global policy data repository to describe the policies;
sending policy data to the plurality of computer assets, the policy data at least describing the policies in the global policy data repository;
wherein the method is performed by one or more computer devices that implement an analyzer component

16. The method of Claim 15,
wherein the analyzer component is one of a plurality of analyzers, each configured to perform the steps of Claim 16 with respect to a different plurality of computer assets;
wherein the global policy data repository is shared amongst at least the plurality of analyzers.
17. The method of Claim 15, further comprising:
identifying one or more of the policies based on determining, from the message information, that a condition described by a system-level policy exists;
generating one or more asset-level policies comprising logic for identifying messages to block or redirect in view of the described condition; and

updating the global policy data to include the generated one or more asset-level policies.

18. The method of Claim 15, further comprising:
identifying a distributed attack on a computer system comprising the plurality of computer assets based on collectively analyzing the message information;
generating a first policy comprising logic for identifying messages involved in the distributed attack; and
updating the global policy data to describe the first policy.
19. The method of Claim 15, further comprising:
based on the message information, the analyzer component identifying an attack that is occurring at a first computer asset;
generating a first policy comprising logic for identifying messages involved in the attack at least a second asset of the plurality of computer assets, the analyzer component having not yet received message information from the second asset indicating that the second asset has received messages involved in the attack;
updating the global policy data to describe the first policy.
20. The computer system of Claim 1, wherein the plurality of computer assets is configured to automatically remove the policies based on a time criteria.