IN THE CLAIMS

The following listing of claims will replace all prior version, and listings, of claims in the application.

1. (Currently amended) A non-transitory computer-readable storage medium that stores one or more sequences of instructions for enforcing security constraints against a network without impacting business workflows, which when executed by one or more processors, cause:

programmatically dividing, without human intervention, the network into a set of restrictive subnetworks; ~~and~~

one or more agents, executing on a plurality of nodes of the network, enforcing the security constraints by requiring a process, which requests access to an asset stored on a node of said plurality of nodes, to possess a security credential associated with a particular restrictive subnetwork to which said node belongs for access to said asset to be granted; and

the one or more agents enforcing the security constraints by requiring a requestor, associated with the process, to possess security credentials associated with all restrictive subnetworks over which the requestor must traverse to gain access to the particular restrictive subnetwork, wherein said all restrictive subnetworks over which the requestor must traverse includes at least two restrictive subnetworks.

2. (Original) The non-transitory computer-readable storage medium of Claim 1,

wherein the set of restrictive subnetworks is determined based upon a risk model designed to minimize risk to the network.

3. (Original) The non-transitory computer-readable storage medium of Claim 1, wherein a composition of nodes comprised within each restrictive network of said set of restrictive networks is determined using a risk model designed to minimize risk to the network.

4. (Original) The non-transitory computer-readable storage medium of Claim 1, wherein at least one of the one or more nodes belongs to two or more restrictive subnetworks.

5. (Cancelled).

6. (Original) The non-transitory computer-readable storage medium of Claim 1, wherein said security constraints are enforced by the one or more agents at one or more of a credential layer, a networking layer, and an application layer.

7 (Currently amended) A non-transitory computer-readable storage medium that stores one or more sequences of instructions for enforcing security constraints against a network without impacting business workflows, which when executed by one or more processors, cause:

programmatically dividing, without human intervention, the network into a set of

restrictive subnetworks; and

one or more agents, executing on a plurality of nodes of the network, enforcing the security constraints by requiring a process, which requests access to an asset stored on a node of said plurality of nodes, to possess a security credential associated with a particular restrictive subnetwork to which said node belongs for access to said asset to be granted~~The non-transitory computer-readable storage medium of Claim 1~~,

wherein the one or more agents enforcing the security constraints comprises:

upon determining that a certain amount of risk exists in granting the process access to said asset, requiring a user initiating said process to be authenticated by one or more users dynamically chosen contemporaneously with said process requesting access to said asset,

wherein a random set of one or more users is dynamically chosen for each process requesting access to any resource when the certain amount of risk exists in granting said each process access to said resource.

8. (Original) The non-transitory computer-readable storage medium of Claim 1, wherein execution of the one or more sequences of instructions further cause:

the one or more agents enforcing one or more restrictions on the access granted to said process in accessing said asset.

9. (Original) The non-transitory computer-readable storage medium of Claim 8,

wherein the one or more restrictions comprise limiting an amount of time the asset may be accessed, limiting an amount of the asset which may be accessed, limiting a set of actions which may be performed against or using said asset, or liming how many times a particular action may be performed against said asset.

10. (Original) The non-transitory computer-readable storage medium of Claim 1, wherein execution of the one or more sequences of instructions further cause:

upon the one or more agents determining that there exists a magnitude of risk beyond a specified level in granting the process access to said asset, then one or more agents performing:

the one or more agents dynamically replicating a counterfeit asset having similar features to said asset and dissimilar content to said asset; and

the one or more agents granting the process access to said counterfeit asset without granting the process access to the asset.

11. (Currently amended) A system for enforcing security constraints against a network without impacting business workflows, comprising:

one or more processors; and

one or more non-transitory computer-readable storage mediums storing one or more sequences of instructions, which when executed, cause:

programmatically dividing, without human intervention, the network into a set of restrictive subnetworks; ~~and~~

one or more agents, executing on a plurality of nodes of the network, enforcing the security constraints by requiring a process, which requests access to an asset stored on a node of said plurality of nodes, to possess a security credential associated with a particular restrictive subnetwork to which said node belongs for access to said asset to be granted; and

the one or more agents enforcing the security constraints by requiring a requestor, associated with the process, to possess security credentials associated with all restrictive subnetworks over which the requestor must traverse to gain access to the particular restrictive subnetwork, wherein said all restrictive subnetworks over which the requestor must traverse includes at least two restrictive subnetworks.

12. (Original) The system of Claim 11, wherein the set of restrictive subnetworks is determined based upon a risk model designed to minimize risk to the network.

13. (Original) The system of Claim 11, wherein a composition of nodes comprised within each restrictive network of said set of restrictive networks is determined using a risk model designed to minimize risk to the network.

14. (Original) The system of Claim 11, wherein at least one of the one or more nodes belongs to two or more restrictive subnetworks.

15. (Cancelled).

16. (Original) The system of Claim 11, wherein said security constraints are enforced by the one or more agents at one or more of a credential layer, a networking layer, and an application layer.

17. (Currently amended) A system for enforcing security constraints against a network without impacting business workflows, comprising:

one or more processors; and

one or more non-transitory computer-readable storage mediums storing one or more sequences of instructions, which when executed, cause:

programmatically dividing, without human intervention, the network into a set of restrictive subnetworks;

one or more agents, executing on a plurality of nodes of the network, enforcing the security constraints by requiring a process, which requests access to an asset stored on a node of said plurality of nodes, to possess a security credential associated with a particular restrictive subnetwork to which said node belongs for access to said asset to be granted~~The system of Claim 11~~, wherein the one or more agents enforcing the security constraints comprises:

upon determining that a certain amount of risk exists in granting the process access to said asset, requiring a user initiating said process

to be authenticated by one or more users dynamically chosen contemporaneously with said process requesting access to said asset,

wherein a random set of one or more users is dynamically chosen for each process requesting access to any resource when the certain amount of risk exists in granting said each process access to said resource.

18. (Original) The system of Claim 11, wherein execution of the one or more sequences of instructions further cause:

the one or more agents enforcing one or more restrictions on the access granted to said process in accessing said asset.

19. (Original) The system of Claim 18, wherein the one or more restrictions comprise limiting an amount of time the asset may be accessed, limiting an amount of the asset which may be accessed, limiting a set of actions which may be performed against or using said asset, or liming how many times a particular action may be performed against said asset.

20. (Original) The system of Claim 11, wherein execution of the one or more sequences of instructions further cause:

upon the one or more agents determining that there exists a magnitude of risk beyond a specified level in granting the process access to said asset, then one or more agents performing:

the one or more agents dynamically replicating a counterfeit asset having similar features to said asset and dissimilar content to said asset; and

the one or more agents granting the process access to said counterfeit asset without granting the process access to the asset.

21. (Currently amended) A method for enforcing security constraints against a network without impacting business workflows, comprising:

programmatically dividing, without human intervention, the network into a set of restrictive subnetworks; ~~and~~

one or more agents, executing on a plurality of nodes of the network, enforcing the security constraints by requiring a process, which requests access to an asset stored on a node of said plurality of nodes, to possess a security credential associated with a particular restrictive subnetwork to which said node belongs for access to said asset to be granted; and

the one or more agents enforcing the security constraints by requiring a requestor, associated with the process, to possess security credentials associated with all restrictive subnetworks over which the requestor must traverse to gain access to the particular restrictive subnetwork, wherein said all restrictive subnetworks over which the requestor must traverse includes at least two restrictive subnetworks.

22. (New) The method of Claim 21, wherein the set of restrictive subnetworks is

determined based upon a risk model designed to minimize risk to the network.

23. (New) The method of Claim 21, wherein a composition of nodes comprised within each restrictive network of said set of restrictive networks is determined using a risk model designed to minimize risk to the network.