

Claims

1. A method comprising:
running an application in a host operating system;
detecting an access to a network resource by the application;
determining whether the network resource is a trusted network resource or an untrusted network resource; and
in response to determining that the network resource is an untrusted network resource:
activating, by the host operating system, a container that is isolated from the host operating system and configured to run a version of the application; and
allowing, by the host operating system, the version of the application running in the container to access the untrusted network resource.
2. The method as recited in claim 1, further comprising allowing the version of the application running in the container to access one or more additional untrusted network resources and preventing the application running in the container from accessing trusted network resources.
3. The method as recited in claim 1 or claim 2, further comprising detecting an access to a file or an application by the host operating system and, in response to determining that the file or the application is an untrusted network resource, allowing the file or the application to be opened within the container.
4. The method as recited in any one of claims 1 to 3, wherein the container includes an instance of the host operating system and a kernel that is separate and isolated from a kernel of the host operating system.
5. The method as recited in any one of claims 1 to 4, further comprising receiving at least one policy that includes at least an enumerated list of trusted network resources, wherein determining whether the network resource is a trusted network resource or an untrusted network resource comprises comparing the network resource against the enumerated list of trusted network resources, the enumerated list of trusted network resources being identified based on one or more of a file type of the network resource, a network location associated with the network resource, or an application type that is attempting to access the network resource.
6. The method as recited in any one of claims 1 to 5, wherein the container is activated for a user that is logged on to the host operating system, the method further comprising determining that a different user is logged on to the host operating system and

activating, for the different user, a different container that is isolated from the host operating system and the container.

7. The method as recited in claim any one of claims 1 to 6, further comprising determining that the access to the network resource is requested over an untrusted network interface and, in response to determining that the access to the network resource is requested over the untrusted network interface:

restricting network communications for the application in the host operating system to a virtual private network (VPN) interface;

allowing the version of the application running in the container to perform network communications over the untrusted network interface; and

indicating to a network stack of the container that network communications for the container are isolated to the untrusted network interface.

8. The method as recited in any one of claims 1 to 7, further comprising intercepting, by the host operating system, a response to a web proxy prompt for user credentials and inserting one or more user credentials into the response to the web proxy prompt without communicating the one or more user credentials to the container.

9. The method as recited in any one of claims 1 to 8, further comprising scanning one or more untrusted network resources that are accessed in the container and using antivirus software in the host operating system to assign one or more risk levels to the one or more untrusted network resources and quarantine, clean, or delete one of the one or more untrusted network resources if the assigned risk level indicates that the untrusted network resource is malicious.

10. The method as recited in any one of claims 1 to 9, further comprising monitoring activity associated with the untrusted network resource in the container and updating local policy at the host operating system based on the monitored activity.

11. The method as recited in any one of claims 1 to 10, wherein the application is a web application and the untrusted network resource is a web page.

12. The method as recited in any one of claims 1 to 11, wherein the container is activated for network resource communications over a first network communication interface, the method further comprising activating a second container for network resource communications over a second network communication interface.

13. A device comprising:

one or more processors; and

one or more computer-readable storage media storing computer-readable

instructions that are executable by the one or more processors to perform operations comprising:

- running a web application on a host operating system of the device;
- detecting access to a network resource by the web application;
- determining that the network resource is an untrusted resource by comparing the network resource to a policy received from a management and monitoring service that is located remotely from the device;
- in response to determining that the network resource is an untrusted network resource:
 - activating, by the host operating system, a container that is isolated from the host operating system and configured to run a version of the web application;
 - allowing, by the host operating system, the version of the web application running in the container to access the untrusted network resource;
 - allowing the version of the web application running in the container to access one or more additional untrusted network resources; and
 - preventing the version of the web application running in the container from accessing trusted network resources.

14. The device as recited in claim 13, the operations further comprising detecting an update to the host operating system and, in response to detecting the update to the host operating system, deleting the container and creating a new container that reflects one or more updated binaries of the host operating system.

15. The device as recited in claim 13 or claim 14, wherein the host operating system is configured to determine that the network resource and the one or more additional untrusted network resources are untrusted based on one or more of a file type of the network resource, a network location associated with the network resource, an application type that is attempting to access the network resource, anti-virus scanning of the network resource, or based on consulting a cloud-based service that maintains a list of malicious network resources.