ENTERPRISE BROWSER SYSTEM

BACKGROUND

Web browser are among the most widely used computer software applications. Organizations, including commercial business enterprises and government bodies, are increasingly dependent on the use of web browsers by those who work on their behalf. Organizations that wish to exercise control over web browsers, such as to audit their use and prevent them from downloading malware or transmitting sensitive information outside of the organization, are typically forced to implement various measures that are external to web browsers, such as on computers that host web browsers and on network infrastructure through which web browsers communicate. Unfortunately, such measures are often costly and complex to configure and manage, lack visibility to all aspects of internal web browser operation, can impede web browser users from accomplishing their work tasks efficiently, and are too often thwarted by successful attempts to bypass them.

SUMMARY

In one aspect of the present disclosure, a web browser is provided including a browser and rendering engine configured to send and receive data via a computer network, and a policy engine configured to implement one or more policies configured to control any aspect of the web browser, the data, a computer that hosts the web browser, and any devices that are accessible to the computer, where the web browser is configured as an executable file that is created by compiling computer software instructions that implement the browser and rendering engine and the policy engine, and where the web browser is configured to require a user of the web browser to be authenticated and one or more policies to be validated before the web browser is allowed to perform one or more predefined operations, wherein the web browser is configured to receive the policies via the computer network, wherein the policies are encrypted, before they are sent to the web browser via the computer network, for decryption using a decryption key that is uniquely associated with an identity that is associated with the user of the web browser, and wherein the decryption key is provided to the web browser via the computer network after the user is authenticated.

In an example each of the policies includes one or more policy conditions and one or more policy enforcement actions that are performed when the policy conditions are met.

In an example the web browser is configured to receive the policies from a source that is external to web browser, where the policies are encrypted for decryption using a decryption key that is uniquely associated with an identity that is associated with the

user of the web browser, and where the decryption key is provided to the web browser after the user is authenticated.

In an example the web browser is configured to receive from the source browser settings associated with the authenticated user, where the browser settings are encrypted for decryption using the decryption key.

In an example the web browser is configured to at least partially evaluate any of the policies that apply to the data in parallel to receiving the data.

In an example the web browser is configured to at least partially evaluate any of the policies that apply to the data in parallel to receiving the data and in parallel to providing any portion of the data to the browser and rendering engine.

In an example any of the policies includes a policy condition that relates to a category associated with a website accessed by the web browser.

In an example any of the policies includes a policy condition that relates to a risk level associated with a website accessed by the web browser.

In an example any of the policies includes a policy condition that relates to any characteristic of the computer that hosts the web browser.

In an example any of the policies includes a policy condition that relates to any characteristic of identity of the user of the web browser.

In an example any of the policies includes a policy condition that relates to any characteristic of identity of a network that is accessible to the web browser.

In an example any of the policies includes a policy condition that relates to a source of a Uniform Resource Locator (URL) that is provided to the web browser.

In an example any of the policies includes a policy enforcement action that requires performing any of data loss prevention (DLP) techniques, antivirus techniques, or antimalware techniques to the data.

In an example any of the policies includes a policy enforcement action that requires changing or otherwise manipulating the data prior to rendering the data or providing the data to the user.

CLAIMS

What is claimed is:

1. A web browser comprising:

a browser and rendering engine configured to send and receive data via a computer network; and

a policy engine configured to implement one or more policies configured to control any aspect of the web browser, the data, a computer that hosts the web browser, and any devices that are accessible to the computer,

wherein the web browser is configured as an executable file that is created by compiling computer software instructions that implement the browser and rendering engine and the policy engine, and

wherein the web browser is configured to require a user of the web browser to be authenticated and one or more policies to be validated before the web browser is allowed to perform one or more predefined operations,

wherein the web browser is configured to receive the policies via the computer network,

wherein the policies are encrypted, before they are sent to the web browser via the computer network, for decryption using a decryption key that is uniquely associated with an identity that is associated with the user of the web browser, and

wherein the decryption key is provided to the web browser via the computer network after the user is authenticated.

2. The web browser according to claim 1 wherein each of the policies includes one or more policy conditions and one or more policy enforcement actions that are performed when the policy conditions are met.

3. The web browser according to claim 1 wherein the web browser is configured to receive from the source browser settings associated with the authenticated user, wherein the browser settings are encrypted for decryption using the decryption key.

4. The web browser according to claim 1 wherein the web browser is configured to at least partially evaluate any of the policies that apply to the data in parallel to receiving the data.

5. The web browser according to claim 1 wherein the web browser is configured to at least partially evaluate any of the policies that apply to the data in parallel to receiving the data and in parallel to providing any portion of the data to the browser and rendering engine.

6. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to a category associated with a website accessed by the web browser.

7. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to a risk level associated with a website accessed by the web browser.

8. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to any characteristic of the computer that hosts the web browser.

9. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to any characteristic of identity of the user of the web browser.

10. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to any characteristic of identity of a network that is accessible to the web browser.

11. The web browser according to claim 1 wherein any of the policies includes a policy condition that relates to a source of a Uniform Resource Locator (URL) that is provided to the web browser.

12. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires performing any of data loss prevention (DLP) techniques, antivirus techniques, or antimalware techniques to the data.

13. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires changing or otherwise manipulating the data prior to rendering the data or providing the data to the user.

14. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires, prior to rendering the data or providing the data to the user, converting the data from a first format to at least second format that eliminates a portion of the data, and then converting the converted data to the first format.

15. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires controlling client-side user interactions with a website.

16. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires hiding a browser tab that is closed by the user and showing the hidden browser tab when the user next attempts to access a website or other content associated with the hidden browser tab.

17. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires disabling a predefined application programming interface (API) of the web browser.

18. The web browser according to claim 1 wherein any of the policies includes a policy enforcement action that requires any of disabling, hiding, or masking a predefined element of a webpage.

19. The web browser according to claim 1 and further comprising an auditor configured to record any actions attempted or performed by the user when using the web browser.

20. The web browser according to claim 1 and further comprising an auditor configured to record any actions attempted or performed by the web browser when the web browser is used by the user.

21. The web browser according to claim 1 and further comprising an auditor configured to record any network activity detectable by the web browser.

22. The web browser according to claim 1 wherein the web browser is specifically configured to operate with one or more target applications.

23. The web browser according to claim 22 wherein the policies are specifically adapted for use with the one or more target applications.

24. The web browser according to claim 1 wherein any of the policies are defined and enforced using robotic process automation (RPA) techniques.

25. The web browser according to claim 1 wherein

the web browser is configured to implement multiple different profiles that are isolated from one another,

each of the profiles has its own data including policies, cookies, cache, and local storage, and

the different profiles are associated with any of different and concurrently-displayed browser tabs, different and concurrently-executing processes, and different and concurrently-executing browser instances.