CLAIMS

1. A malware detection method comprising employing at least one hardware processor of a computer system to:

determine a plurality of primary feature values characterizing a software entity executing on the computer system;

execute a plurality of feature processors to determine a plurality of derived feature values according to the plurality of primary feature values, wherein a selected feature processor of the plurality of feature processors is configured to determine a selected derived feature value according to a selected subset of the plurality of primary feature values;

in response to a failure to determine the selected derived feature value, supply a surrogate value to replace the missing selected derived feature value; and

determine whether the software entity is malicious according to the plurality of derived feature values and further according to the surrogate value.

2. The method of claim 1, wherein supplying the surrogate value comprises employing the at least one hardware processor to calculate the surrogate value according to a reference value determined by another feature processor executing on a device distinct from the computer system.

3. The method of claim 2, wherein supplying the surrogate value comprises calculating the surrogate value according to a statistic of a plurality of reference values, the plurality of reference values determined by other feature processors executing on devices distinct from the computer system.

4. The method of claim 1, wherein supplying the surrogate value comprises selectively retrieving the surrogate value from a database storing a plurality of reference values determined by other feature processors executing on devices distinct from the computer system.

5. The method of claim 4, comprising selecting the surrogate value from the plurality of reference values according to a current state of the computer system.

6. The method of claim 4, comprising selecting the surrogate value from the plurality of reference values according to a device type of the computer system.

7. The method of claim 1, wherein supplying the surrogate value comprises:

employing the at least one hardware processor of the computer system to transmit a data request to a remote security server, the data request formulated according to an indicator of a current state of the computer system; and

in response to transmitting the data request, receiving the surrogate value from the remote security server.

8. The method of claim 7, wherein the data request includes at least one value of the plurality of primary feature values.

9. The method of claim 1, wherein each feature processor of the plurality of feature processors comprises a neural network trained to determine a likelihood that the software entity is malicious according to a respective subset of the plurality of primary feature values.

10. A computer system having at least one hardware processor configured to execute:

a feature extractor configured to determine a plurality of primary feature values characterizing a software entity executing on the computer system;

a plurality of feature processors configured to determine a plurality of derived feature values according to the plurality of primary feature values, wherein a selected feature processor of the plurality of feature processors is configured to determine a selected derived feature value according to a selected subset of the plurality of primary feature values;

a data substitution module connected to the plurality of feature processors and configured to, in response to a failure to determine the selected feature value supply a surrogate value to replace the missing selected derived feature value; and

a synthesizer module configured to determine whether the software entity is malicious according to the plurality of derived feature values and further according to the surrogate value.

11. The computer system of claim 10, wherein supplying the surrogate value comprises employing the at least one hardware processor to calculate the surrogate value according to a reference value determined by another feature processor executing on a device distinct from the computer system.

12. The computer system of claim 11, wherein supplying the surrogate value comprises calculating the surrogate value according to a statistic of a plurality of reference values, the plurality of reference values determined by other feature processors executing on devices distinct from the computer system.

13. The computer system of claim 10, wherein supplying the surrogate value comprises selectively retrieving the surrogate value from a database storing a plurality of

reference values determined by other feature processors executing on devices distinct from the computer system.

14. The computer system of claim 13, wherein the data substitution module is configured to select the surrogate value from the plurality of reference values according to a current state of the computer system.

15. The computer system of claim 13, wherein the data substitution module is configured to select the surrogate value from the plurality of reference values according to a device type of the computer system.

16. The computer system of claim 10, wherein supplying the surrogate value comprises:

transmitting a data request to a remote security server, the data request formulated according to an indicator of a current state of the computer system; and

in response to transmitting the data request, receiving the surrogate value from the remote security server.

17. The computer system of claim 16, wherein the data request includes at least one value of the plurality of primary feature values.

18. The computer system of claim 10, wherein each feature processor of the plurality of feature processors comprises a neural network trained to determine a likelihood that the software entity is malicious according to a respective subset of the plurality of primary feature values.

19. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a computer system, cause the computer system to perform malware detection comprising:

determining a plurality of primary feature values characterizing a software entity executing on the computer system;

executing a plurality of feature processors to determine a plurality of derived feature values according to a plurality of primary feature values, wherein a selected feature processor of the plurality of feature processors is configured to determine a selected derived feature value according to a selected subset of the plurality of primary feature values;

in response to a failure to determine the selected derived feature value, supplying a surrogate value to replace the missing selected derived feature value; and

determining whether the software entity is malicious according to the plurality of derived feature values and further according to the surrogate value.