CLAIMS

What is claimed is:

1. A host system comprising at least one processor configured to execute:
a hypervisor configured to expose a virtual machine;
a process evaluator executing within the virtual machine;
a memory introspection engine executing outside the virtual machine; and
a process-scoring module, wherein:
the process evaluator is configured to:
determine whether an evaluated process executing within the virtual machine performs an action, and
in response, when the evaluated process performs the action, transmit a first process evaluation indicator to the process-scoring module, the first process evaluation indicator determined for the evaluated process;
the memory introspection engine is configured to:
intercept a call to an operating system function, to detect a launch of a protected process executing within the virtual machine, wherein the operating system function is configured to add the protected process to a list of processes executing within the virtual machine, and
in response to detecting the launch,
determine whether the evaluated process attempts to modify a memory page of the protected process, and
in response, when the evaluated process attempts to modify the memory page,
transmit a second process evaluation indicator to the process-scoring module, the second process evaluation indicator determined for the evaluated process; and
the process-scoring module is configured to:
receive the first and second process evaluation indicators, and

in response, determine whether the evaluated process is malicious according to the first and second process evaluation indicators.

2. The host system of claim 1, wherein the memory introspection engine is further configured to:

in response to detecting the launch of the protected process, send an indicator of the protected process to a security application executing within the virtual machine, and

in response, receive from the security application an indicator of the memory page.

3. The host system of claim 1, wherein the process evaluator comprises a user-level process evaluator executing at user level of processor privilege, the user-level process evaluator configured to determine whether the evaluated process performs the action.

4. The host system of claim 1, wherein the process evaluator comprises a kernel-level process evaluator executing at kernel level of processor privilege, the kernel-level process evaluator configured to determine whether the evaluated process performs the action.

5. The host system of claim 1, wherein the process evaluator comprises a system call evaluator configured to intercept a system call performed by the evaluated process.

6. The host system of claim 1, wherein the process-scoring module executes within the virtual machine.

7. The host system of claim 1, wherein the process-scoring module executes outside the virtual machine.

8. The host system of claim 1, wherein determining whether the evaluated process is malicious comprises determining an aggregate score according to a first score and a second score, the first and second scores determined at a security server according to

the first and second process evaluation indicators, respectively, wherein the security server is configured to perform anti-malware transactions with a plurality of computer systems including the host system.

9. The host system of claim 1, wherein determining whether the evaluated process is malicious comprises determining an aggregate score according to a weighted sum of a first score and a second score, the first and second scores determined according to the first and second process evaluation indicators, respectively, and wherein the process scoring module is further configured to receive from a security server a first weight and a second weight, the first weight multiplying the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, and wherein the security server is configured to perform anti-malware transactions with a plurality of computer systems including the host system.

10. The host system of claim 1, wherein the protected process includes the process scoring module.

11. The host system of claim 1, wherein the protected process forms a part of a security application comprising the process evaluator.

12. A non-transitory computer-readable medium encoding instructions which, when executed on a host system comprising at least one processor, cause the host system to form:
a hypervisor configured to expose a virtual machine;
a process evaluator executing within the virtual machine;
a memory introspection engine executing outside the virtual machine; and
a process-scoring module, wherein:
the process evaluator is configured to:
determine whether an evaluated process executing within the virtual machine performs an action, and

in response, when the evaluated process performs the action, transmit a first process evaluation indicator to the process-scoring module, the first process evaluation indicator determined for the evaluated process;

the memory introspection engine is configured to:

intercept a call to an operating system function, to detect a launch of a protected process executing within the virtual machine, wherein the operating system function executes within the virtual machine and is configured to add the protected process to a list of processes executing within the virtual machine, and

in response to detecting the launch,

determine whether the evaluated process attempts to modify a memory page of the protected process, and

in response, when the evaluated process attempts to modify the memory page,

transmit a second process evaluation indicator to the process-scoring module, the second process evaluation indicator determined for the evaluated process; and

the process-scoring module is configured to:

receive the first and second process evaluation indicators, and

in response, determine whether the evaluated process is malicious according to the first and second process evaluation indicators.

13. The non-transitory computer-readable medium of claim 12, wherein the memory introspection engine is further configured to:

in response to detecting the launch of the protected process, send an indicator of the protected process to a security application executing within the virtual machine, and

in response, receive from the security application an indicator of the memory page.

14. The non-transitory computer-readable medium of claim 12, wherein the process evaluator comprises a user-level process evaluator executing at user level of

processor privilege, the user-level process evaluator configured to determine whether the evaluated process performs the action.

15. The non-transitory computer-readable medium of claim 12, wherein the process evaluator comprises a kernel-level process evaluator executing at kernel level of processor privilege, the kernel-level process evaluator configured to determine whether the evaluated process performs the action.

16. The non-transitory computer-readable medium of claim 12, wherein the process evaluator comprises a system call evaluator configured to intercept a system call performed by the evaluated process.

17. The non-transitory computer-readable medium of claim 12, wherein the process-scoring module executes within the virtual machine.

18. The non-transitory computer-readable medium of claim 12, wherein the process-scoring module executes outside the virtual machine.

19. The non-transitory computer-readable medium of claim 12, wherein determining whether the evaluated process is malicious comprises determining an aggregate score according to a first score and a second score, the first and second scores determined at a security server according to the first and second process evaluation indicators, respectively, wherein the security server is configured to perform anti-malware transactions with a plurality of computer systems including the host system.

20. The non-transitory computer-readable medium of claim 12, wherein determining whether the evaluated process is malicious comprises determining an aggregate score according to a weighted sum of a first score and a second score, the first and second scores determined according to the first and second process evaluation indicators, respectively, and wherein the process scoring module is further configured to receive from a security server a first weight and a second weight, the first weight multiplying

the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, and wherein the security server is configured to perform anti-malware transactions with a plurality of computer systems including the host system.

21. The non-transitory computer-readable medium of claim 12, wherein the protected process includes the process-scoring module.

22. The non-transitory computer-readable medium of claim 12, wherein the protected process forms a part of a security application configured to execute the process evaluator.

23. A method comprising:

employing at least one processor of a host system to receive a first process evaluation indicator determined for an evaluated process, the evaluated process executing within a virtual machine exposed by a hypervisor executing on the host system;

employing the at least one processor to receive a second process evaluation indicator determined for the evaluated process; and

in response to receiving the first and second process evaluation indicators, employing the at least one processor to determine whether the evaluated process is malicious according to the first and second process evaluation indicators;

wherein determining the first process evaluation indicator comprises employing a process evaluator executing within the virtual machine to determine whether the evaluated process performs a first action,

and wherein determining the second process evaluation indicator comprises employing a memory introspection engine executing outside the virtual machine to determine whether the evaluated process performs a second action.

24. A method comprising:

employing at least one processor of a host system to execute a memory introspection engine, the memory introspection engine executing outside a virtual machine exposed by a hypervisor executing on the host system, wherein executing the memory introspection engine comprises detecting a launch of a process executing within the virtual machine;

in response to the memory introspection engine detecting the launch of the process, employing the at least one processor to determine a first and a second process evaluation indicators of the process; and

in response to determining the first and second evaluation indicators, employing the at least one processor to determine whether the process is malicious according to the first and second process evaluation indicators.

CLAIMS

1. A host system comprising at least one hardware processor configured to execute:

a hypervisor configured to expose a virtual machine;

a process evaluator executing within the virtual machine;

a memory introspection engine executing outside the virtual machine; and

a process-scoring module, wherein:

the process evaluator is configured to:

determine whether an evaluated process executing within the virtual machine performs an action and

in response, when the evaluated process performs the action, transmit a first process evaluation indicator to the process-scoring module, the first process evaluation indicator determined for the evaluated process;

the memory introspection engine is configured to:

intercept a call to an operating system function, to detect a launch of a protected process executing within the virtual machine, wherein the operating system function is configured to add the protected process to a list of processes executing within the virtual machine, and

in response to detecting the launch,

determine whether the evaluated process attempts to modify a memory page of the protected process, and

in response, when the evaluated process attempts to modify the memory page, transmit a second process evaluation indicator to the process-scoring module, the second process evaluation indicator determined for the evaluated process; and

the process-scoring module is configured to:

receive a first weight and a second weight from a security server configured to perform anti-malware transactions with a plurality of computer systems including the host system, receive the first and second process evaluation indicators, and

in response, determine whether the evaluated process is malicious according to the first and second process evaluation indicators, wherein determining whether the evaluated process is malicious comprises determining a weighted sum of a first score and a second score, the first weight multiplying the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, wherein the first and second scores are determined according to the first and second process evaluation indicators, respectively.

2. The host system of claim 1, wherein the memory introspection engine is further configured to:

in response to detecting the launch of the protected process, send an indicator of the protected process to a security application executing within the virtual machine, and in response, receive from the security application an indicator of the memory page.

3. The host system of claim 1, wherein the process evaluator comprises a user-level process evaluator executing at user level of processor privilege, the user-level process evaluator configured to determine whether the evaluated process performs the action.

4. The host system of claim 1, wherein the process evaluator comprises a kernel-level process evaluator executing at kernel level of processor privilege, the kernel-level process evaluator configured to determine whether the evaluated process performs the action.

5. The host system of claim 1, wherein the process evaluator comprises a system call evaluator configured to intercept a system call performed by the evaluated process.

6. The host system of claim 1, wherein the process-scoring module executes within the virtual machine.

7. The host system of claim 1, wherein the process-scoring module executes outside the virtual machine.

8. The host system of claim 1, wherein the protected process includes the process scoring module.

9. The host system of claim 1, wherein the protected process forms a part of a security application comprising the process evaluator.

10. A non-transitory computer-readable medium encoding instructions which, when executed on a host system comprising at least one processor, cause the host system to form:

a hypervisor configured to expose a virtual machine;

a process evaluator executing within the virtual machine;

a memory introspection engine executing outside the virtual machine; and

a process-scoring module, wherein:

the process evaluator is configured to:

determine whether an evaluated process executing within the virtual machine performs an action, and

in response, when the evaluated process performs the action, transmit a first process evaluation indicator to the process-scoring module, the first process evaluation indicator determined for the evaluated process;

the memory introspection engine is configured to:

intercept a call to an operating system function, to detect a launch of a protected process executing within the virtual machine, wherein the operating system function executes within the

virtual machine and is configured to add the protected process to a list of processes executing within the virtual machine, and

in response to detecting the launch,

determine whether the evaluated process attempts to modify a memory page of the protected process, and

in response, when the evaluated process attempts to modify the memory page, transmit a second process evaluation indicator to the process-scoring module, the second process evaluation indicator determined for the evaluated process; and

the process-scoring module is configured to:

receive a first weight and a second weight from a security server configured to perform anti-malware transactions with a plurality of computer systems including the host system, receive the first and second process evaluation indicators, and

in response, determine whether the evaluated process is malicious according to the first and second process evaluation indicators, wherein determining whether the evaluated process is malicious comprises determining a weighted sum of a first score and a second score, the first weight multiplying the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, wherein the first and second scores are determined according to the first and second process evaluation indicators, respectively.

11. The non-transitory computer-readable medium of claim 10, wherein the memory introspection engine is further configured to:

in response to detecting the launch of the protected process, send an indicator of the protected process to a security application executing within the virtual machine, and

in response, receive from the security application an indicator of the memory page.

12. The non-transitory computer-readable medium of claim 10, wherein the process evaluator comprises a user-level process evaluator executing at user level of processor privilege, the user-level process evaluator configured to determine whether the evaluated process performs the action.

13. The non-transitory computer-readable medium of claim 10, wherein the process evaluator comprises a kernel-level process evaluator executing at kernel level of processor privilege, the kernel-level process evaluator configured to determine whether the evaluated process performs the action.

14. The non-transitory computer-readable medium of claim 10, wherein the process evaluator comprises a system call evaluator configured to intercept a system call performed by the evaluated process.

15. The non-transitory computer-readable medium of claim 10, wherein the process-scoring module executes within the virtual machine.

16. The non-transitory computer-readable medium of claim 10, wherein the process-scoring module executes outside the virtual machine.

17. The non-transitory computer-readable medium of claim 10, wherein the protected process includes the process-scoring module.

18. The non-transitory computer-readable medium of claim 10, wherein the protected process forms a part of a security application configured to execute the process evaluator.

19. A method comprising:

employing at least one hardware processor of a host system to receive a first weight and a second weight from a security server configured to perform anti-malware transactions with a plurality of computer systems including the host system;

employing the at least one hardware processor to receive a first process evaluation indicator determined for an evaluated process, the evaluated process executing within a virtual machine exposed by a hypervisor executing on the host system, wherein determining the first process evaluation indicator comprises employing a process evaluator executing within the virtual machine to determine whether the evaluated process performs a first action;

employing the at least one hardware processor to receive a second process evaluation indicator determined for the evaluated process, wherein determining the second process evaluation indicator comprises employing a memory introspection engine executing outside the virtual machine to determine whether the evaluated process performs a second action; and

in response to receiving the first and second process evaluation indicators, employing the at least one hardware processor to determine whether the evaluated process is malicious according to the first and second process evaluation indicators, wherein determining whether the evaluated process is malicious comprises determining a weighted sum of a first score and a second score, the first weight multiplying the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, wherein the first and second scores are determined according to the first and second process evaluation indicators, respectively.

20. A method comprising:

employing at least one hardware processor of a host system to receive a first weight and a second weight from a security server configured to perform anti-malware transactions with a plurality of computer systems including the host system;

employing the at least one hardware processor to execute a memory introspection engine, the memory introspection engine executing outside a virtual machine exposed by a hypervisor executing on the host system, wherein executing the memory introspection engine comprises detecting a launch of a process executing within the virtual machine;

in response to the memory introspection engine detecting the launch of the process, employing the at least one hardware processor to determine a first and a second process evaluation indicators of the process; and

in response to determining the first and second evaluation indicators, employing the at least one hardware processor to determine whether the process is malicious according to the first and second process evaluation indicators, wherein determining whether the evaluated process is malicious comprises determining a weighted sum of a first score and a second score, the first weight multiplying the first score in the weighted sum, and the second weight multiplying the second score in the weighted sum, wherein the first and second scores are determined according to the first and second process evaluation indicators, respectively.