CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

under the control of one or more computer systems configured with executable instructions,

receiving a request to provision a virtual machine for a user;

selecting a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtaining a cryptographic measurement of the one or more resources on the selected host computing device; and

determining whether to provide the user with access to the virtual machine on the host computing device based at least in part on a comparison of the cryptographic measurement to one or more reference values.

2. The computer implemented method of claim 1, wherein determining whether to provide the user with access to the virtual machine further comprises:

receiving a selection of a configuration of the host computing device from the user;

determining an approved cryptographic measurement associated with the selected configuration of the host computing device; and

verifying that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device.

3. The computer implemented method of claim 1, wherein determining whether to provide the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

4. The computer implemented method of claim 1, wherein determining whether to provide the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

5. The computer implemented method of claim 1, wherein the one or more reference values further comprise:

a list of approved cryptographic measurements generated by a trusted third party and attested to by the trusted third party.

6. The computer implemented method of claim 1, further comprising:

compiling a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

providing the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

7. The computer implemented method of claim 6, wherein the list of approved cryptographic measurements is published by the trusted third party to be accessible over a network by a plurality of users.

8. The computer implemented method of claim 4, wherein the list of approved cryptographic measurements is provided by the user along with the request to provision the virtual machine.

9. The computer implemented method of claim 1, wherein the hash measurement is based at least in part on one or more of:

values associated with a basic input/output system (BIOS) of the host computing device;

configuration of a hypervisor of the host computing device;

configuration of a boot operating system of the virtual machine;

values in one or more hardware configuration registers; or

firmware in a peripheral component interconnect (PCI) card.

10. A computing system, comprising:

at least one processor; and

memory including instructions that, when executed by the processor, cause the computing system to:

receive a request to provision a virtual machine for a user;

select a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtain a cryptographic measurement of the one or more resources on the selected host computing device; and

determine whether to provide the user with access to the virtual machine on the host computing device based at least in part on a comparison of the cryptographic measurement to one or more reference values.

11. The computing system of claim 10, wherein determining whether to provide the user with access to the virtual machine further comprises:

receiving a selection of a configuration of the host computing device from the user;

determining an approved cryptographic measurement associated with the selected configuration of the host computing device; and

verifying that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device.

12. The computing system of claim 10, wherein determining whether to provide the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

13. The computing system of claim 10, wherein determining whether to provide the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

14. The computing system of claim 10, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

compile a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

provide the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

15. The computing system of claim 14, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

determine that at least one of a plurality of host computing devices has been patched or updated; and

update the list of approved cryptographic measurements with a new cryptographic measurement to account for the patch or update to the host computing devices.

CLAIMS

What is claimed is:

1. A non-transitory computer readable storage medium storing one or more sequences of instructions, which when executed by one or more processors to cause a computing system to:

receive a request to provision a virtual machine for a customer, the request received from a customer of a service provider hosting a multitenant computing environment;

select a host computing device from a plurality of host computing devices to host the virtual machine, the selected host computing device including one or more resources for executing the virtual machine;

provision the virtual machine on the selected host computing device;

generate a hash measurement of a configuration of the one or more resources on the selected host computing device;

obtain, from the customer, an indication of whether the configuration of the one or more resources is acceptable for hosting the virtual machine, the indication being based at least in part on a comparison between the hash measurement and a list of approved hash measurements; and

launch the virtual machine on the selected host computing device in response to the indication that the configuration of the one or more resources is acceptable.

2. The non-transitory computer readable storage medium of claim 1, wherein the list of approved hash measurements is a trusted list attested to by a trusted third party.

3. The non-transitory computer readable storage medium of claim 1, wherein the hash measurement is based at least in part on one or more of:

values associated with a basic input/output system (BIOS) of the host computing device;

configuration of a hypervisor of the host computing device;

configuration of a boot operating system of the virtual machine;

values in one or more hardware configuration registers; or

firmware in a peripheral component interconnect (PCI) card.

4. The non-transitory computer readable storage medium of claim 1, further comprising instructions executed by one or more processors to cause a computing system to:

provide the hash measurement to the customer in response to the request to provision the virtual machine.

5. A computer implemented method, comprising:

receiving a request to provision a virtual machine for a user;

selecting a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtaining a cryptographic measurement of the one or more resources on the selected host computing device;

receiving a selection of a configuration of the host computing device from the user;

determining an approved cryptographic measurement associated with the selected configuration of the host computing device;

verifying that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device; and

providing the user with access to the virtual machine on the host computing device.

6. The computer implemented method of claim 5, wherein providing the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

7. The computer implemented method of claim 5, wherein providing the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

8. The computer implemented method of claim 7, wherein the list of approved cryptographic measurements is provided by the user along with the request to provision the virtual machine.

9. The computer implemented method of claim 5, wherein the approved cryptographic measurement is generated by a trusted third party and attested to by the trusted third party.

10. The computer implemented method of claim 5, further comprising:

compiling a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

providing the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

11. The computer implemented method of claim 10, further comprising:

determining that at least one of a plurality of host computing devices has been patched or updated; and

updating the list of approved cryptographic measurements with a new cryptographic measurement to account for the patch or update to the host computing devices.

12. The computer implemented method of claim 10, wherein the list of approved cryptographic measurements is published by the trusted third party to be accessible over a network by a plurality of users.

13. The computer implemented method of claim 5, wherein the cryptographic measurement is based at least in part on one or more of:

values associated with a basic input/output system (BIOS) of the host computing device;

configuration of a hypervisor of the host computing device;

configuration of a boot operating system of the virtual machine;

values in one or more hardware configuration registers; or

firmware in a peripheral component interconnect (PCI) card.

14. A computing system, comprising:

at least one processor; and

memory including instructions that, when executed by the processor, cause the computing system to:

receive a request to provision a virtual machine for a user;

select a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtain a cryptographic measurement of the one or more resources on the selected host computing device;

receive a selection of a configuration of the host computing device from the user;

determine an approved cryptographic measurement associated with the selected configuration of the host computing device;

verify that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device; and

provide the user with access to the virtual machine on the host computing device.

15. The computing system of claim 14, wherein providing the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

16. The computing system of claim 14, wherein providing the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

17. The computing system of claim 16, wherein the list of approved cryptographic measurements is provided by the user along with the request to provision the virtual machine.

18. The computing system of claim 14, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

compile a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

provide the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

19. The computing system of claim 18, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

determine that at least one of a plurality of host computing devices has been patched or updated; and

update the list of approved cryptographic measurements with a new cryptographic measurement to account for the patch or update to the host computing devices.

20. The computing system of claim 18, wherein the list of approved cryptographic measurements is published by the trusted third party to be accessible over a network by a plurality of users.

CLAIMS

What is claimed is:

1. A non-transitory computer readable storage medium storing one or more sequences of instructions, which when executed by one or more processors to cause a computing system to:

receive a request to provision a virtual machine for a customer, the request received from a customer of a service provider hosting a multitenant computing environment;

select a host computing device from a plurality of host computing devices to host the virtual machine, the selected host computing device including one or more resources for executing the virtual machine;

provision the virtual machine on the selected host computing device;

generate a hash measurement of a configuration of the one or more resources on the selected host computing device;

obtain, from the customer, an indication of whether the configuration of the one or more resources is acceptable for hosting the virtual machine, the indication being based at least in part on a comparison between the hash measurement and a list of approved hash measurements; and

launch the virtual machine on the selected host computing device in response to the indication that the configuration of the one or more resources is acceptable.

2. The non-transitory computer readable storage medium of claim 1, wherein the list of approved hash measurements is a trusted list attested to by a trusted third party.

3. The non-transitory computer readable storage medium of claim 1, wherein the hash measurement is based at least in part on one or more of:

values associated with a basic input/output system (BIOS) of the host computing device;

configuration of a hypervisor of the host computing device;

configuration of a boot operating system of the virtual machine;

values in one or more hardware configuration registers; or

firmware in a peripheral component interconnect (PCI) card.

4. The non-transitory computer readable storage medium of claim 1, further comprising instructions executed by one or more processors to cause a computing system to:

provide the hash measurement to the customer in response to the request to provision the virtual machine.

5. A computer implemented method, comprising:

receiving a request to provision a virtual machine for a user;

selecting a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtaining a cryptographic measurement of the one or more resources on the selected host computing device;

receiving a selection of a configuration of the host computing device from the user;

determining an approved cryptographic measurement associated with the selected configuration of the host computing device;

verifying that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device; and

providing the user with access to the virtual machine on the host computing device.

6. The computer implemented method of claim 5, wherein providing the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

7. The computer implemented method of claim 5, wherein providing the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

8. The computer implemented method of claim 7, wherein the list of approved cryptographic measurements is provided by the user along with the request to provision the virtual machine.

9. The computer implemented method of claim 5, wherein the approved cryptographic measurement is generated by a trusted third party and attested to by the trusted third party.

10. The computer implemented method of claim 5, further comprising:

compiling a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

providing the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

11. The computer implemented method of claim 10, further comprising:

determining that at least one of a plurality of host computing devices has been patched or updated; and

updating the list of approved cryptographic measurements with a new cryptographic measurement to account for the patch or update to the host computing devices.

12. The computer implemented method of claim 10, wherein the list of approved cryptographic measurements is published by the trusted third party to be accessible over a network by a plurality of users.

13. The computer implemented method of claim 5, wherein the cryptographic measurement is based at least in part on one or more of:

values associated with a basic input/output system (BIOS) of the host computing device;

configuration of a hypervisor of the host computing device;

configuration of a boot operating system of the virtual machine;

values in one or more hardware configuration registers; or

firmware in a peripheral component interconnect (PCI) card.

14. A computing system, comprising:

at least one processor; and

memory including instructions that, when executed by the processor, cause the computing system to:

receive a request to provision a virtual machine for a user;

select a host computing device for hosting the virtual machine, the host computing device including one or more resources for executing the virtual machine;

obtain a cryptographic measurement of the one or more resources on the selected host computing device;

receive a selection of a configuration of the host computing device from the user;

determine an approved cryptographic measurement associated with the selected configuration of the host computing device;

verify that the cryptographic measurement matches the approved cryptographic measurement associated with the selected configuration of the host computing device; and

provide the user with access to the virtual machine on the host computing device.

15. The computing system of claim 14, wherein providing the user with access to the virtual machine further comprises:

providing the cryptographic measurements to the user in response to the request to provision the virtual machine;

receiving an indication from the user, indicating whether the cryptographic measurement is approved by the user; and

launching the virtual machine on the host computing device in response to receiving an indication that the cryptographic measurement is approved.

16. The computing system of claim 14, wherein providing the user with access to the virtual machine further comprises:

retrieving a list of approved cryptographic measurements;

comparing the cryptographic measurement to the list of approved cryptographic measurements to determine whether the one or more resources on the selected host computing device are acceptable for hosting the virtual machine; and

launching the virtual machine on the selected host computing device in response to determining that the one or more resources are acceptable.

17. The computing system of claim 16, wherein the list of approved cryptographic measurements is provided by the user along with the request to provision the virtual machine.

18. The computing system of claim 14, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

compile a list of approved cryptographic measurements for a plurality of configurations for host computing devices; and

provide the list of approved cryptographic measurements to a trusted third party to be attested to by the trusted third party.

19. The computing system of claim 18, wherein the memory further comprises instructions executed by the at least one processor to cause the computing system to:

determine that at least one of a plurality of host computing devices has been patched or updated; and

update the list of approved cryptographic measurements with a new cryptographic measurement to account for the patch or update to the host computing devices.

20. The computing system of claim 18, wherein the list of approved cryptographic measurements is published by the trusted third party to be accessible over a network by a plurality of users.