CLAIMS

1. A method comprising:

applying static security features to a first instance of an application operating at a first edge computing environment of a system;

applying first dynamic security features to the first instance of the application, wherein the first dynamic security features are dynamically determined based on dynamic information specific to operation of the first instance of the application at the first edge computing environment;

instantiating a second instance of the application at a second edge computing environment of the system, including:

identifying the first dynamic security features; and

applying the static security features and the first dynamic security features to the second instance of the application at the second edge computing environment; and

redirecting at least some traffic from the first instance of the application to the second instance of the application.

2. The method of claim 1, wherein the system includes a third instance of an application operating at a third edge computing environment of the system, further comprising:

applying the static security features to the third instance of an application; and

applying third dynamic security features to the third instance of the application, wherein the third dynamic security features are based on dynamic information specific to operation of the third instance of the application at the third edge computing environment.

3. The method of any preceding claim, further comprising:

removing the first instance of the application from the first edge computing environment.

4. The method of any preceding claim, further comprising, prior to instantiating the second instance of the application:

evaluating performance data related to the first instance of the application or the first edge computing environment; and

determining that the performance data exceeds a threshold;

wherein instantiating the second instance of the application is based on determining that the performance data exceeds the threshold.

5. The method of any preceding claim, wherein the first dynamic security features comprise one or more of: DDoS mitigation features, firewall analysis features, user analysis features, and data loss prevention features.

6. The method of any preceding claim, wherein applying the first dynamic security features comprises determining that the first instance of the application is experiencing a cyberattack, identifying source-identifying data for attacking devices, dynamically blocking traffic from the attacking devices, and applying security protections for the detected cyberattack, wherein the source-identifying data comprises one or more of:

user identifying information comprising one or more of a username, user identifier, or account identifier;

device identifying information comprising one or more of a device name, IP address, or media access control (MAC) address; or

originating network/region information comprising one or more of network trace information or packet header information.

7. The method of any preceding claim, further comprising:

periodically storing the first dynamic security features at a core system storage;

wherein applying the first dynamic security features to the second instance of the application at the second edge computing environment comprises copying the first dynamic security features from the core system storage.

8. The method of any preceding claim, wherein the second edge computing environment comprises a secured computing environment that prevents untrusted entities from inspecting the secured computing environment, further comprising:

identifying an attacker of the first application instance;

wherein redirecting at least some traffic from the first instance of the application to the second instance of the application comprising redirecting only traffic from the identified attacker.

9. The method of any preceding claim, wherein applying the first dynamic security features to the second instance of the application at the second edge computing environment comprises:

determining a first component of the second edge computing environment to perform filtering of the at least some traffic;

filtering the at least some traffic with the first component;

monitoring performance data for the second edge computing environment; and

based on the performance data for the second edge computing environment, causing a second component of the second edge computing environment to begin filtering the at least some traffic.

10. A system, comprising:

at least one processor; and

memory, operatively connected to the processor, the memory storing computer executable instructions that, when executed by the at least one processor, cause the system to perform a method, the method comprising:

applying static security features to a first instance of an application operating at a first edge computing environment of a system;

applying first dynamic security features to the first instance of the application, wherein the first dynamic security features are dynamically determined based on dynamic information specific to operation of the first instance of the application at the first edge computing environment;

instantiating a second instance of the application, including:

identifying the first dynamic security features; and

applying the static security features and the first dynamic security features to the second instance of the application; and

redirecting at least some traffic from the first instance of the application to the second instance of the application.

11. The system of claim 10, wherein the system includes a third instance of an application operating at a third edge computing environment of the system, the method further comprising:

applying the static security features to the third instance of an application; and

applying third dynamic security features to the third instance of the application, wherein the third dynamic security features are based on dynamic information specific to operation of the third instance of the application at the third edge computing environment.

12. The system of claim 10 or 11, wherein the method further comprises:

removing the first instance of the application from the first edge computing environment.

13. The system of any one of claims 10 to 12, wherein the method further comprises, prior to instantiating the second instance of the application:

evaluating performance data related to the first instance of the application or the first edge computing environment; and

determining that the performance data exceeds a threshold;

wherein instantiating the second instance of the application is based on determining that the performance data exceeds the threshold.

14. The system of any one of claims 10 to 13, wherein the first dynamic security features comprise one or more of: DDoS mitigation features, firewall analysis features, user analysis features, and data loss prevention features.

15. The system of any one of claims 10 to 14, wherein applying the first dynamic security features comprises determining that the first instance of the application is experiencing a cyberattack, identifying source-identifying data for attacking devices, dynamically blocking traffic from the attacking devices, and applying security protections for the detected cyberattack, wherein the source-identifying data comprises one or more of:

user identifying information comprising one or more of a username, user identifier, or account identifier;

device identifying information comprising one or more of a device name, IP address, or media access control (MAC) address; or

originating network/region information comprising one or more of network trace information or packet header information.

16. The system of any one of claims 10 to 15, wherein the method further comprises:

periodically storing the first dynamic security features at a core system storage;

wherein applying the first dynamic security features to the second instance of the application comprises copying the first dynamic security features from the core system storage.

17. The system of any one of claims 10 to 16, wherein instantiating a second instance of the application comprises instantiating the second instance of the application at a second edge computing environment that comprises a secured computing environment that prevents untrusted entities from inspecting the secured computing environment.

18. The system of claim 17, wherein the method further comprises:

identifying an attacker of the first application instance;

wherein redirecting at least some traffic from the first instance of the application to the second instance of the application comprising redirecting only traffic from the identified attacker.

19. A method comprising:

applying static security features to a first instance of an application operating at a first edge computing environment of a system;

operating the first instance of the application at the first edge computing environment;

collecting dynamic information relating to operating the first instance of the application at the first edge computing environment;

applying first dynamic security features to the first instance of the application, wherein the first dynamic security features are dynamically determined based on the collected dynamic information;

evaluating performance data related to the first instance of the application or the first edge computing environment; and

determining that the performance data exceeds a threshold;

instantiating, based on determining that the performance data exceeds the threshold, a second instance of the application at a second edge computing environment of the system, including:

identifying the first dynamic security features; and

applying the static security features and the first dynamic security features to the second instance of the application at the second edge computing environment; and

redirecting at least some traffic from the first instance of the application to the second instance of the application.

20. The method of claim 19, wherein applying the first dynamic security features comprises determining that the first instance of the application is experiencing a cyberattack, identifying source-identifying data for attacking devices, dynamically blocking traffic from the attacking devices, and applying security protections for the detected cyberattack, wherein the source-identifying data comprises one or more of:

user identifying information comprising one or more of a username, user identifier, or account identifier;

device identifying information comprising one or more of a device name, IP address, or media access control (MAC) address; or

originating network/region information comprising one or more of network trace information or packet header information.