

CLAIMS

1. A system, comprising:
 - one or more processors; and
 - 5 memory comprising computer executable instructions that, when executed by the one or more processors, cause the system to:
 - operate, by a service provider, an application programming interface to which requests are submittable over a network, the request originating from a network not operated by the service provider; and
 - 10 for each first request of at least a plurality of requests submitted to the application programming interface, process the first request by at least:
 - using a key to perform one or more cryptographic operations on data involved in processing the first request, wherein the key is maintained in a first zone and wherein the key is encrypted with a customer key and
 - 15 the customer key is encrypted with a domain key, wherein the domain key is stored in a cryptographic module in the first zone; and transmitting, across a network, a second request to a service that causes the service to perform one or more operations on the data in encrypted form wherein the service is in a second zone, different from the first zone, and lacks
 - 20 access to the key and being configured to be independently configured to process the second request.

2. The system of claim 1, wherein: the system is operated as part of a first instance of the service type provided by the service provider; and the service is operated as part of a second instance of the service type provided by the service provider.

5

3. The system of claim 1, wherein the application programming interface is a web service interface.

4. The system of claim 1, wherein: at least some of the plurality of requests are transmitted by different entities; and each different entity corresponds to an account of the service.

5. The system of claim 1, wherein: the executable instructions further cause the system to selectively determine whether to perform the one or more cryptographic operations when processing requests; and the plurality of requests are a subset of a set of requests processed by the system, the subset including requests for which the system has selectively determined to perform the one or more cryptographic operations.

6. The system of claim 1, wherein the executable instructions further cause the system to select the service from a plurality of services configured to process the first request.

7. The system of claim 1, wherein: the second request to the service causes the service to perform one or more operations on unencrypted data and

provide, to the system, a result of performing the one or more operations and the data in encrypted form; wherein using the key to perform the one or more cryptographic operations includes decrypting the data in encrypted form; and the executable instructions further cause the system to perform
5 one or more operations on a collection of data comprising the unencrypted data and the decrypted data.

8. The system of claim 1, wherein the service is operated by a first organizational entity that is different from the service provider that operates
10 the system.

9. The system of claim 1, wherein the executable instructions further cause the system to restrict access by the service to the data in encrypted form based at least in part on an analysis of the application programming interface
15 request.

10. A computer-implemented method, comprising: under the control of one or more computer systems configured with executable instructions, receiving, from a requestor at a network address of the one or more computer
20 systems, a plurality of requests submitted to an application programming interface to perform one or more operations; and processing the application programming interface request by at least: transmitting, over the network, a second request to a service operated that is configured to be independently configured to perform the one or more operations, the second request being
25 configured to cause the service to perform one or more service operations

on encrypted data, the encrypted data being encrypted under a key that is inaccessible to the service, wherein the key is maintained in a first zone and wherein the service is in a second zone, different from the first zone; and using the key to perform one or more cryptographic operations in connection
5 with the encrypted data, and wherein the key is encrypted with a customer key and the customer key is encrypted with a domain key, wherein the domain key is stored in a cryptographic module in the first zone.

11. The computer-implemented method of claim 10, wherein: the one or more
10 cryptographic operations include encryption of data to obtain the encrypted data; and the one or more service operations include persistent storage of the encrypted data.

12. The computer-implemented method of claim 10, wherein the network
15 address is a public Internet protocol address.

13. The computer-implemented method of claim 10, wherein the method further comprises selecting the service from a plurality of services each independently configured to perform the one or more operations.

20 14. The computer-implemented method of claim 10, wherein performing the one or more cryptographic operations includes transmitting, over the network to a cryptography service, a request that causes the cryptography service to perform one or more other cryptographic operations using cryptographic

information that is inaccessible to both the one or more computer systems and the service.

15. The computer-implemented method of claim 10, wherein the network

5 address is associated with a string that is usable for obtaining the network address from a domain name service, the string being unassociated with a network address for the service by any domain name service.

16. The system of claim 1, wherein the memory further includes instructions

10 that, when executed by the one or more processors cause the system to analyze the request to determine whether to restrict access by the first data storage service to a subset of the data in encrypted form.

17. A system, comprising: a first data storage service comprising a plurality of

15 data storage devices and a first web service interface configured to receive web service requests transmitted to the first web service interface, the first data storage service being configured to process the web service requests transmitted to the first web service interface using the plurality of data storage devices; and a second data storage service, where first data storage
20 service is implemented with computing resources in a first set of one or more facilities operated by a computing resource service provider and the second data storage service is implemented with computing resources in a second set of one or more facilities that is geographically distinct from the first set of one or more facilities and operated by the computing resource
25 service provider and the first data storage service is configured in

accordance with a first set of regulations associated with a first legal jurisdiction and the second data storage service is configured in accordance with a second set of regulations that is different from the first set of regulations and associated with a second legal jurisdiction, the second data storage service comprising a second web service interface, the second data storage service configured to operate as a proxy to the first data storage service by at least: receiving, at the second web service interface, a request from a requestor to store data, the request originating from a network not operated by the service provider; encrypting the data using a cryptographic key inaccessible to the first data storage service, wherein the key is encrypted with a customer key and the customer key is encrypted with a domain key, wherein the domain key is stored in a cryptographic module in the first data storage service; transmitting the encrypted data to the first data storage service for persistent storage on behalf of the requestor; and maintaining access to the cryptographic key while preventing access to the cryptographic key by the first data storage service.

18. The system of claim 17, wherein both the first web service interface and the second web service interface are each publicly addressable interfaces in a public communications network.

19. The system of claim 17, wherein the second data storage service is configured to encrypt the data without requiring the requestor to specify that the data should be encrypted.

20. The system of claim 17, wherein the second data storage service is further configured to: receive, to the second web service interface, a request to retrieve the data; obtain the encrypted data from the first data storage service; use the key to decrypt the encrypted data; and provide the decrypted data.

21. The system of claim 17, wherein the first data storage service and second data storage service are implemented in different legal jurisdictions.

22. One or more non-transitory computer-readable storage media having collectively stored therein computer executable instructions that, when executed by one or more processors of a computer system, cause the computer system to: provide an application programming interface accessible at a network address; receive, at the application programming interface, at least one application programming interface request, from a requestor, to perform one or more operations on a set of data, the application programming interface request originating from a network in a first zone that is not associated with the network address and governed by different regulations; and fulfill the received application programming interface request, at least in part by: causing at least a subset of the set of data to be encrypted under a key kept inaccessible to a remote service, wherein the key is encrypted with a customer key and the customer key is encrypted with a domain key, wherein the domain key is stored in a cryptographic module in the requestor platform; and utilizing the remote

service in a second zone, different from the first zone and operated by a service provider distinct from the requestor to perform at least a subset of the one or more operations on the set of data such that, for the subset of the set of data, the remote service has access to the subset of the set of data
5 only in encrypted form.

23. The one or more non-transitory computer-readable storage media of claim 22, wherein: the network address is a public Internet protocol address; and utilizing the remote service includes transmitting a request to the remote
10 service addressed to a public Internet protocol address of the remote service.

24. The one or more non-transitory computer-readable storage media of claim 22, wherein the remote service is independently configured to perform a
15 requested operation as indicated in the application programming interface request for the requestor.

25. The one or more non-transitory computer-readable storage media of claim 22, wherein: the computer executable instructions further cause the
20 computer system to analyze the application programming interface request to determine whether to restrict access by the remote service to the subset of the data in encrypted form; and the remote service only having access to the subset of the data in encrypted form as a result of determining to restrict access by the remote service to the subset of the data in encrypted form.

26. The one or more non-transitory computer-readable storage media of claim 25, wherein: as a result of determining to restrict access by the remote service to the subset, the instructions further cause the computer system to determine, based at least in part on analysis of the application programming interface request, an encryption key; and restricting access by the remote service includes encrypting at least a portion of the subset using the determined encryption key.
27. The one or more non-transitory computer-readable storage media of claim 22, wherein: a plurality of services that include the remote service are configured to be utilized by the computer system for fulfilling the application programming interface request; and the computer executable instructions further cause the computer system to select, from the plurality of services, the remote service based at least in part on a configuration setting specific to the requestor.
28. The one or more non-transitory computer-readable storage media of claim 22, wherein: the computer executable instructions further cause the computer system to encrypt the subset of the set of data using the key; and utilizing the remote service to perform one or more operations includes submitting a storage request to the remote service to store the set of data.
29. A system, comprising:
- one or more processors; and

memory including computer executable instructions that, when executed by the one or more processors, cause the system to:

provide an application programming interface accessible at a network address;

5 receive data in connection with a request from a first zone to perform one or more operations submitted to the application programming interface;

analyze the data to identify a subset of data that meets one or more criteria of one or more data policies;

10 modify the subset of data in accordance with the one or more data policies by at least encrypting the subset of data using a cryptographic key inaccessible to a remote service that is in a second zone different from the first zone and is independently capable of processing the request to perform the one or more operations, to form a modified subset of data, wherein the cryptographic key is determined based at least in part on a type of the
15 subset of data; and

wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key; and provide the modified subset of data to the remote service.

20 30. The system of claim 29, wherein the computer executable instructions further cause the system to at least:
provide one or more notifications corresponding to meeting the one or more criteria, or

perform enhanced logging for the subset identified.

31. The system of claim 29, wherein the computer executable instructions

further include computer executable instructions that cause the system to:

5 obtain an encrypted cryptographic key;

decrypt the encrypted cryptographic key to form the cryptographic key; and

as a result of transmission of the modified subset of data to the remote
service, destroy the cryptographic key.

10 32. The system of claim 29, wherein:

the computer executable instructions further cause the system to receive,
through the application programming interface, user-defined rules for
modifying data; and

the computer executable instructions that cause the system to modify the
15 subset of data cause the system to modify the data in accordance with the
user-defined rules.

33. The system of claim 29, wherein:

20 the computer executable instructions that cause the system to analyze the
data includes computer executable instructions that cause the system to
detect, in the data, one or more instances of a data type specified as
sensitive; and

the subset of data includes the one or more instances of the data type specified as sensitive.

34. The system of claim 29, wherein the computer executable instructions

5 further cause the system to provide a second subset of the data received to the remote service without modifying the second subset.

35. The system of claim 29, wherein the computer executable instructions

further cause the system to:

10 receive a second request whose fulfillment includes retrieval of the subset of data;

obtain the modified subset of data from the remote service;

reverse modification of the modified subset of data to form a regenerated subset of data; and

15 fulfill the second request using the regenerated subset of data.

36. A computer-implemented method, comprising:

under the control of one or more computer systems having one or more hardware processors and memory including executable instructions,

20 receiving from a first zone at an application programming interface proxy to a remote service, a request to process data whose fulfillment involves utilization of the remote service;

analyzing the data to make a determination whether the data implicates one or more data policies;

processing the data in accordance with the determination at least in part by modifying the data according to the one or more data policies implicated prior to
5 utilization of the remote service, by at least encrypting the data to form encrypted data; and

utilizing the remote service, in a second zone different from the first zone, and that is independently capable to process the request, the remote service lacking a cryptographic key usable to decrypt the encrypted data, wherein the
10 cryptographic key is determined based at least in part on a type of a subset of data and wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key.

37. The computer-implemented method of claim 36, comprising:

15 obtaining an encrypted data key;
decrypting the encrypted data key to form the cryptographic key; and
as a result of the remote service to process the request, destroy the cryptographic key.

20 38. The computer-implemented method of claim 36, wherein the request is received at a private Internet protocol address of the application programming interface proxy.

39. The computer-implemented method of claim 36, wherein the request to process the data is a request to store the data.

40. The computer-implemented method of claim 36, further comprising:

5 receiving, at the application programming interface proxy, one or more user-defined criteria for the one or more data policies; and
generating the determination is based at least in part on the one or more user-defined criteria.

10 41. The computer-implemented method of claim 36, further comprising:

receiving, at the application programming interface, a second request to process second data whose fulfillment involves utilization of the remote service; and
preventing the second data from being transmitted to the remote service as
15 a result of the second data satisfying one or more criteria of the one or more data policies.

42. One or more non-transitory computer-readable storage media having

collectively stored thereon executable instructions that, when executed by
20 one or more processors of a system, cause the system to:
provide an application programming interface proxy to a remote service;

cause one or more data loss prevention policies on data received from a first zone through the application programming interface proxy to be enforced at the remote service by at least:

5 identifying a subset of the data received that satisfies one or more data loss prevention criteria of the one or more data loss prevention policies; and

performing one or more actions on the subset identified in accordance with the one or more data loss prevention criteria, the one or more actions including:

10 modifying data in the subset, at least by encrypting the data in the subset, to form modified data; and

providing the modified data to the remote service in a second zone different from the first zone and that is independently capable to process a request and lacks access to a cryptographic key usable to decrypt the modified data, wherein the cryptographic key is determined based at least in part on a type of the subset of data and wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key.

20

43. The one or more non-transitory computer-readable storage media of claim 42, wherein:
the system is operated by a computing resource service provider; and

the application programming interface proxy is available to multiple customers of the computing resource service provider at one or more public network addresses.

5 44. The one or more non-transitory computer-readable storage media of claim 42, wherein the application programming interface proxy and remote service are implemented in separate facilities.

45. The one or more non-transitory computer-readable storage media of claim
10 42, wherein the one or more data loss prevention policies are programmatically configurable through the application programming interface proxy.

46. The one or more non-transitory computer-readable storage media of claim
15 42, wherein the application programming interface proxy and the remote service are accessible by different uniform resource locators.

47. The one or more non-transitory computer-readable storage media of claim
20 42, wherein performing the one or more actions further includes:
encrypting the cryptographic key to form an encrypted data key; and
providing the encrypted data key to the remote service, wherein the remote service is unable to decrypt the encrypted data key.

48. The system of claim 29, wherein the data is received from a requestor that is different from the system.

49. A system, comprising:

5 one or more computer-readable storage mediums having stored thereon a set of computer executable instructions, which if performed by one or more processors, cause the system to:

 operate an application programming interface to which requests are submittable over a network;

10 for each first request of at least a plurality of requests submitted to the application programming interface, process the first request by at least:

 using a key to perform one or more cryptographic operations on data involved in processing the first request, wherein the key is

 maintained in a first zone, and wherein the key is encrypted with a

15 customer key and the customer key is encrypted with a domain key and the domain key is stored in a cryptographic module in the first zone; and

 transmitting, across a network, a second request to a service that causes the service to perform one or more operations on the data in encrypted form, the service in a second zone, different from the first zone

20 that lacks access to the key and being configured to be independently capable of processing the second request;

 wherein the executable instructions further cause the system to selectively determine whether to perform the one or more cryptographic operations when

processing requests, wherein the plurality of requests are a subset of a set of requests processed by the system, the subset including requests for which the system has selectively determined to perform the one or more cryptographic operations.

5

50. The system of claim 49, wherein:

the system is operated as part of a first instance of a service type provided by the service provider; and

the service is operated as part of a second instance of the service type

10 provided by the service provider.

51. The system of claim 49 or claim 50, wherein the application programming interface is a web service interface.

15 52. The system of any one of claims 49, 50 or 51, wherein:

at least some of the plurality of requests are transmitted by different entities;

and

each different entity corresponds to an account of the service.

20 53. The system of any one of claims 49 to 52, wherein the executable

instructions further cause the system to select the service from a plurality of services capable of being used in processing the first request.

54. The system of any one of claims 49 to 53, wherein:

the second request to the service causes the service to perform one or more operations on unencrypted data and provide, to the system, a result of performing the one or more operations and the data in encrypted form;

5 wherein using the key to perform the one or more cryptographic operations includes decrypting the data in encrypted form; and

the executable instructions further cause the system to perform one or more operations on a collection of data comprising the unencrypted data and the decrypted data.

10

55. The system of any of claims 49 to 54, wherein the service is operated by a first organizational entity that is different from a second organizational entity that operates the system.

15 56. The system of any of claims 49 to 55, wherein the executable instructions further cause the system to restrict access by the service to the data in encrypted form based at least in part on an analysis of the application programming interface request.

20 57. A computer-implemented method, comprising:

receiving, from a requestor at a network address of one or more computer systems configured with executable instructions, a plurality of requests

submitted to an application programming interface to perform one or more operations; and

processing a first request of the plurality of requests submitted to the application programming interface request by at least:

- 5 transmitting, over a network, a second request to a service that is configured to be independently capable of performing the one or more operations, the second request being configured to cause the service to perform one or more service operations on encrypted data, the encrypted data being encrypted under a key that is inaccessible to the service,
- 10 wherein the key is maintained in a first zone and wherein the services is in a second zone, different from the first zone; and using the key to perform one or more cryptographic operations in connection with the encrypted data and wherein the key is encrypted with a customer key and the customer key is encrypted with a domain key, wherein the domain key is stored in a
- 15 cryptographic module in the first zone, and wherein the executable instructions further cause the one or more computer systems to selectively determine whether to perform the one or more cryptographic operations when processing requests; and the plurality of requests are a subset of a set of requests processed by the one or more computer systems, the subset including requests
- 20 for which the one or more computer systems has selectively determined to perform the one or more cryptographic operations.

58. The computer-implemented method of claim 57, wherein:

the one or more cryptographic operations include encryption of data to obtain the encrypted data; and

the one or more service operations include persistent storage of the encrypted data.

5

59. The computer-implemented method of claim 57 or claim 58, wherein the network address is a public Internet protocol address.

60. The computer-implemented method of any one of claims 57, 58 or 59,
10 wherein the method further comprises selecting the service from a plurality of services each independently capable of performing the one or more operations.

61. The computer-implemented method of any one of claims 57 to 60, wherein
15 performing the one or more cryptographic operations includes transmitting, over the network to a cryptography service, a request that causes the cryptography service to perform one or more other cryptographic operations using cryptographic information that is inaccessible to both the one or more computer systems and the service.

20

62. The computer-implemented method of any one of claims 57 to 61, wherein the network address is associated with a string that is usable for obtaining the network address from a domain name service, the string being

unassociated with a network address for the service by any domain name service.

63. A system, comprising: one or more processors; and memory including

5 computer executable instructions that, when executed by the one or more processors, cause the system to: provide, by a service provider, an application programming interface accessible to one or more customers at a network address in a first zone; receive, by the service provider, data in connection with a request to perform one or more operations submitted to

10 the application programming interface by the one or more customers; analyze, by the service provider, the data to identify, based at least in part on a data type: a subset of data that has the data type and that meets one or more criteria of one or more data policies, wherein an encryption algorithm is selected from a plurality of encryption algorithms based on the data type and

15 security requirement associated with the one or more data policies; modify, by the service provider, the subset of the data in accordance with the one or more data policies by at least encrypting the subset of the data using a cryptographic key inaccessible to a remote service that is independently capable of processing the request to perform the one or more operations,

20 wherein the remote service comprises a set of computer systems that excludes the system and the cryptographic key is not stored in plaintext form when the cryptographic key is stored in the remote service and wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key; and provide, by the service provider, the

modified subset of the data to the remote service, wherein the remote service provides data-related services to customers.

64. The system of claim 63, wherein the computer executable instructions further cause the system to at least: provide one or more notifications
5 corresponding to meeting the one or more criteria, or perform enhanced logging for the subset identified.

65. The system of claim 63, wherein the computer executable instructions further include computer executable instructions that cause the system to: obtain an encrypted cryptographic key; decrypt the encrypted cryptographic
10 key to form the cryptographic key; and as a result of transmission of the modified subset of the data to the remote service, destroy the cryptographic key.

66. The system of claim 63, wherein: the computer executable instructions further cause the system to receive, through the application programming
15 interface, user-defined rules for modifying data; and the computer executable instructions that cause the system to modify the subset of data cause the system to modify the data in accordance with the user-defined rules.

67. The system of claim 63, wherein: the computer executable instructions that
20 cause the system to analyze the data includes computer executable instructions that cause the system to detect, in the data, one or more instances of a data type specified as sensitive; and the subset of the data includes the one or more instances of the data type specified as sensitive.

68. The system of claim 63, wherein the computer executable instructions further cause the system to provide a second subset of the data received to the remote service without modifying the second subset.
69. The system of claim 63, wherein the computer executable instructions
- 5 further cause the system to: receive a second request whose fulfillment includes retrieval of the subset of data; obtain the modified subset of data from the remote service; reverse modification of the modified subset of the data to form a regenerated subset of data; and fulfill the second request using the regenerated subset of data.
- 10 70. The system of claim 63, wherein the data is received from a requestor that is different from the system.
71. A computer-implemented method, comprising: receiving, from a first zone, by a service provider, at an application programming interface proxy to one or more customers at a remote service, a request to process data whose
- 15 fulfillment involves utilization of the remote service, wherein the remote service comprises a set of computer systems that excludes the system and a cryptographic key is not stored in plaintext form when the cryptographic key is stored in the remote service; analyzing, by the service provider, the data to make a determination, based at least in part on a data type: the data
- 20 has the data type and whether the data implicates one or more data policies, wherein an encryption algorithm is selected from a plurality of encryption algorithms based on the data type and security requirement associated with the one or more data policies; processing, by the service provider, the data

in accordance with the determination at least in part by modifying the data according to the one or more data policies implicated prior to utilization of the remote service and the data type, by at least encrypting the data to form encrypted data, wherein the remote service provides data-related services to customers; and utilizing, by a service provider, the remote service in a second zone, different from the first zone and that is independently capable to process the request, the remote service lacking the cryptographic key usable to decrypt the encrypted data, and wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key.

72. The computer-implemented method of claim 71, comprising: obtaining an encrypted data key; decrypting the encrypted data key to form the cryptographic key; and as a result of the remote service to process the request, destroy the cryptographic key.

73. The computer-implemented method of claim 71, wherein the request is received at a private Internet protocol address of the application programming interface proxy.

74. The computer-implemented method of claim 71, wherein the request to process the data is a request to store the data.

75. The computer-implemented method of claim 71, further comprising: receiving, at the application programming interface proxy, one or more user-defined criteria for the one or more data policies; and generating the

determination is based at least in part on the one or more user- defined criteria.

76. The computer-implemented method of claim 71, further comprising:

5 receiving, at the application programming interface, a second request to process second data whose fulfillment involves utilization of the remote service; and preventing the second data from being transmitted to the remote service as a result of the second data satisfying one or more criteria of the one or more data policies.

77. One or more non-transitory computer-readable storage media having

10 collectively stored thereon executable instructions that, when executed by one or more processors of a system, cause the system to: provide, by a service provider, an application programming interface proxy to one or more customers in a first zone at a remote service, wherein the remote service comprises a set of computer systems that excludes the system and a
15 cryptographic key is not stored in plaintext form when the cryptographic key is stored in the remote service; and cause, by the service provider, one or more data loss prevention policies on data received through the application programming interface proxy to be enforced at the remote service by at least: identifying, by the service provider, a subset of the data received,
20 based at least in part on a data type, the data has the data type and that satisfies one or more data loss prevention criteria of the one or more data loss prevention policies, wherein an encryption algorithm is selected from a plurality of encryption algorithms based on the data type and security

requirement associated with the one or more data loss prevention policies;
and performing, by the service provider, one or more actions on the subset
identified in accordance with the one or more data loss prevention criteria,
the one or more actions including: modifying, by the service provider, data in
5 the subset according to the type, at least by encrypting the data in the
subset, to form modified data; and providing, by the service provider, the
modified data to the remote service in a second zone, that is different from
the first zone and that is independently capable to process a request and
lacks access to a cryptographic key usable to decrypt the modified data,
10 wherein the remote service provides data-related services to customers, and
wherein the cryptographic key is encrypted with a customer key and the
customer key is encrypted with a domain key.

78. The one or more non-transitory computer-readable storage media of claim
77, wherein: the system is operated by a computing resource service
15 provider; and the application programming interface proxy is available to
multiple customers of the computing resource service provider at one or
more public network addresses.

79. The one or more non-transitory computer-readable storage media of claim
77, wherein the application programming interface proxy and remote service
20 are implemented in separate facilities.

80. The one or more non-transitory computer-readable storage media of claim
77, wherein the one or more data loss prevention policies are

programmatically configurable through the application programming interface proxy.

81. The one or more non-transitory computer-readable storage media of claim 77, wherein the application programming interface proxy and the remote service are accessible by different uniform resource locators.

82. The one or more non-transitory computer-readable storage media of claim 77, wherein performing the one or more actions further includes: encrypting the cryptographic key to form an encrypted data key; and providing the encrypted data key to the remote service, wherein the remote service is unable to decrypt the encrypted data key.

83. A computer-implemented method, comprising: providing, by a service provider, an application programming interface accessible to one or more customers at a network address in a first zone; receiving, by the service provider, data in connection with a request to perform one or more operations submitted to the application programming interface by one or more customers; analyzing, by the service provider, the data to identify, based at least in part on a data type: a subset of data that has the data type and that meets one or more criteria of one or more data policies; wherein an encryption algorithm is selected from a plurality of encryption algorithms based on data type and security requirement associated with one or more data policies; modifying, by the service provider, the subset of the data in accordance with the one or more data policies by at least encrypting the subset of the data using a cryptographic key inaccessible to a remote

service in a second zone, different from the first zone and that is independently capable of processing the request to perform the one or more operations, wherein the remote service comprises a set of computer systems that excludes the system and the cryptographic key is not stored in plaintext form when the cryptographic key is stored in the remote service and wherein the cryptographic key is encrypted with a customer key and the customer key is encrypted with a domain key; and providing, by the service provider, the modified subset of the data to the remote service, wherein the remote service provides data-related services to customers.

5

10 84. The computer-implemented method of claim 83, further comprising: providing one or more notifications corresponding to meeting the one or more criteria, or performing enhanced logging for the subset identified.

85. The computer-implemented method of claim 83, further comprising: obtaining an encrypted cryptographic key; decrypting the encrypted cryptographic key to form the cryptographic key; and as a result of transmission of the modified subset of the data to the remote service, destroying the cryptographic key.

15

20 86. The computer-implemented method of claim 83, further comprising: causing the system to receive, through the application programming interface, user-defined rules for modifying data; and causing the system to modify the subset of the data cause the system to modify the data in accordance with the user-defined rules.

87. The computer-implemented method of claim 83, wherein analyzing the data includes detecting, in the data, one or more instances of a data type specified as sensitive and the subset of data includes the one or more instances of the data type specified as sensitive.
- 5 88. The computer-implemented method of claim 83, further comprising causing the system to provide a second subset of the data received to the remote service without modifying the second subset.