

U.S. Pat. No. 12,218,934 (Claims 1-30)

Claims 1-10	Claims 11-17	Claims 18-25	Claims 26-30
[1.1] A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:	[11.1] A method implemented on a computer system connected to a network, the method comprising:	[18.1] A computer system is configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:	[26.1] A method implemented on a computer system connected to a network, the method comprising:
[1.2] receive a request to authenticate a client, wherein the request comprises an identifier and a password,	[11.2] receiving a request to authenticate a client, wherein the request comprises an identifier and a password,	[18.2] receive a request to authenticate a client, wherein the request comprises an identifier and a password,	[26.2] receiving a request to authenticate a client, wherein the request comprises an identifier and a password,
[1.3] store, in a multidimensional time-series database, information about the request,	[11.3] storing, in a multidimensional time-series database, information about the request,	[18.2] store, in a multidimensional time-series database, information about the request,	[26.2] storing, in a multidimensional time-series database information about the request,
[1.4] determine whether the password corresponds to a user account identified by the identifier,	[11.4] determining whether the password corresponds to a user account identified by the identifier,	[18.4] determine whether the password corresponds to a user account identified by the identifier,	[26.4] determining whether the password corresponds to a user account identified by the identifier,
[1.5] determine whether an additional verification is required to grant access,	[11.5] determining whether an additional verification is required to grant access,	[18.5] determine whether an additional verification is required to grant access,	[26.5] determining whether an additional verification is required to grant access,
[1.6] wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account, and	[11.6] wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account,	[18.6] wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account, and	[26.6] wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account, and
[1.7] determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is anomalous relative to a	[11.7] determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is anomalous relative to a	[18.7] determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack; and,	[26.7] determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack; and,

U.S. Pat. No. 12,218,934 (Claims 1-30)

Claims 1-10	Claims 11-17	Claims 18-25	Claims 26-30
baseline profile of access requests; and,	baseline profile of access requests; and,		
[1.8] based on the additional verification being required to grant access:	[11.8] to require based on the additional verification being required to grant access:	[18.8] based on the additional verification being required to grant access:	[26.8] based on the additional verification being required to grant access:
[1.9] select an additional verification method from a plurality of verification methods,	[11.9] selecting an additional verification method from a plurality of verification methods,	[18.9] select an additional verification method from a plurality of verification methods,	[26.9] selecting an additional verification method from a plurality of verification methods,
[1.10] cause the client to be prompted to complete the additional verification method, and	[11.10] causing the client to be prompted to complete the additional verification method, and	[18.10] cause the client to be prompted to complete the additional verification method, and	[26.10] causing the client to be prompted to complete the additional verification method, and
[1.11] determine whether the additional verification method has been completed correctly.	[11.11] determining whether the additional verification method has been completed correctly.	[18.11] determine whether the additional verification method has been completed correctly.	[26.11] determining whether the additional verification method has been completed correctly.
[2.1] The computer system of claim 1, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier.	[12.1] The method of claim 11, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier.		
[3.1] The computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.	[13.1] The method of claim 11, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.	[19.1] The computer system of claim 18, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.	[27.1] The method of claim 26, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.
[4.1] The computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises	[14.1] The method of claim 11, wherein determining whether the additional verification is required to grant access further comprises processing an	[20] The computer system of claim 18 wherein determining whether the additional verification is required to grant access further comprises	[28] The method of claim 26, wherein determining whether the additional verification is required to grant access further comprises processing an

U.S. Pat. No. 12,218,934 (Claims 1-30)

Claims 1-10	Claims 11-17	Claims 18-25	Claims 26-30
processing an external threat intelligence feed.	external threat intelligence feed.	processing an external threat intelligence feed.	external threat intelligence feed.
[5.1] The computer system of claim 1, wherein the software instructions further comprise instructions that:	[15.1] The method of claim 11, further comprising:	[21.1] The computer system of claim 18, wherein the software instructions further comprise instructions that:	[29.1] The method of claim 26, further comprising:
[5.2] based on the additional verification being required to grant access:	[15.2] require based on the additional verification being required to grant access:	[21.2] based on the additional verification being required to grant access:	[29.2] based on the additional verification being required to grant access:
[5.3] determine that a probable cyberattack is detected, and	[15.3] determining that a probable cyberattack is detected, and	[21.3] determine that a probable cyberattack is detected, and	[29.3] determining that a probable cyberattack is detected, and
[5.4] provide an alert,	[15.4] delivering an alert,	[21.4] provide an alert,	[29.4] delivering an alert,
[5.5] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	[15.5] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	[21.5] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	[29.5] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and
[5.6] wherein the alert is designated to be provided to an administrator of the network.	[15.6] wherein the alert is designated to be delivered to an administrator of the network.	[21.6] wherein the alert is designated to be provided to an administrator of the network.	[29.6] wherein the alert is designated to be delivered to an administrator of the network.
[6.1] The computer system of claim 5, wherein the alert further includes an indication of where the probable cyberattack may have originated.	[16.1] The method of claim 15, wherein the alert further includes an indication of where the probable cyberattack may have originated.	[22.1] The computer system of claim 21, wherein the alert further includes an indication of where the probable cyberattack may have originated.	[30.1] The method of claim 29, wherein the alert further includes an indication of where the probable cyberattack may have originated.
[7.1] The computer system of claim 5, wherein the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack.	[17.1] The method of claim 15, wherein the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack.	[23.1] The computer system of claim 21, wherein the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack.	
[8.1] The computer system of claim 1, wherein the software instructions further comprise instructions that: deny the request based on determining that the user identification and the			

U.S. Pat. No. 12,218,934 (Claims 1-30)

Claims 1-10	Claims 11-17	Claims 18-25	Claims 26-30
password are not associated with any user account, and deny the request based on determining that the client failed to complete the additional verification method correctly.			
[9.1] The computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines.		[24.1] The computer system of claim 18, wherein the computer system comprises a plurality of physical computing machines.	
[10.1] The computer system of claim 1, wherein the computer system comprises a plurality of virtual computing machines.		[25.1] The computer system of claim 18, wherein the computer system comprises a plurality of virtual computing machines.	