

U.S. Pat. No. 12,231,426 (Claims 1-30)

Claims 1-8	Claims 9-18	Claims 19-25	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:	[9.1] A method implemented on a computer system connected to a network, the method comprising:	[19.1] A computer system 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 a first identifier and a password,	[9.2] receiving a request to authenticate a client, wherein the request comprises a first identifier and a password,	[19.2] receive a request to authenticate a client, wherein the request comprises a first identifier and a password,	[26.2] receiving a request to authenticate a client, wherein the request comprises a first identifier and a password,
[1.3] store, in a multidimensional time-series database, information about the request,	[9.3] storing, in a multidimensional time-series database, information about the request,	[19.3] store, in a multidimensional time-series database, information about the request,	[26.3] storing, in a multidimensional time-series database, information about the request,
[1.4] determine whether the password corresponds to a first user account identified by the first identifier,	[9.4] determining whether the password corresponds to a first user account identified by the first identifier,	[19.4] determine whether the password corresponds to a user account identified by the first identifier,	[26.4] determining whether the password corresponds to a user account identified by the first identifier,
[1.5] determine whether an additional verification is required to grant access,	[9.5] determining whether an additional verification is required to grant access,	[19.5] 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 first user account, and	[9.6] 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 first user account,	[19.6] 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 first user account,	[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,
[1.7] determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous	[9.7] determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous	[19.7] determining, based at least on the historical information, whether the user account is associated with a plurality of previous requests to authenticate, wherein the	[26.7] determining, based at least on the historical information, whether the user account is associated with a plurality of previous requests to authenticate, wherein the

U.S. Pat. No. 12,231,426 (Claims 1-30)

Claims 1-8	Claims 9-18	Claims 19-25	Claims 26-30
request to authenticate comprised a second identifier not associated with the first user account; and,	request to authenticate comprised a second identifier not associated with the first user account; and,	plurality of previous requests to authenticate comprises at least one second identifier not associated with any user account; and,	plurality of previous requests to authenticate comprises at least one second identifier not associated with any user account; and
[1.8] based on the additional verification being required to grant access:	[9.8] based on the additional verification being required to grant access:	[19.8] 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,	[9.9] selecting an additional verification method from a plurality of verification methods,	[19.9] 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	[9.10] causing the client to be prompted to complete the additional verification method, and	[19.10] 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.	[9.11] determining whether the additional verification method has been completed correctly.	[19.11] 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 determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.	[10.1] The method of claim 9, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.	[20.1] The computer system of claim 19, 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.
[3.1] The computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	[11.1] The method of claim 9, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	[21.1] The computer system of claim 19 wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	[28.1] The method of claim 26, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.
[4.1] The computer system of claim 1, wherein the second identifier is associated with a second user account, and wherein	[12.1] The method of claim 9, wherein the second identifier is associated with a second user account, and wherein		

U.S. Pat. No. 12,231,426 (Claims 1-30)

Claims 1-8	Claims 9-18	Claims 19-25	Claims 26-30
the second user account is different from the first user account.	the second user account is different from the first user account.		
[5.1] The computer system of claim 1, wherein the software instructions further comprise instructions that:	[13.1] The method of claim 9, further comprising:	[23.1] The computer system of claim 19, wherein the software instructions further comprise instructions that:	[30.1] The method of claim 29, further comprising:
[5.2] based on the additional verification being required to grant access;	[13.1] based on the additional verification being required to grant access:	[23.1] based on the additional verification being required to grant access:	[30.1] based on the additional verification being required to grant access:
[5.3] determine that a probable cyberattack is detected,	[13.1.a] determining that a probable cyberattack is detected, and	[23.1.a] determine that a probable cyberattack is detected, and provide an alert,	[30.1.a] determining that a probable cyberattack is detected, and delivering an alert,
[5.4] provide an alert	[13.4] delivering an alert,	[23.4] provide an alert,	[30.4] delivering an alert,
[5.5] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and	[13.5] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and	[23.5] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and	[30.5] wherein the alert includes the first 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.	[13.6] wherein the alert is designated to be delivered to an administrator of the network.	[23.6] wherein the alert is designated to be provided to an administrator of the network.	[30.6] 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.	[14.1] The method of claim 13, wherein the alert further includes an indication of where the probable cyberattack may have originated.	[24.1] The computer system of claim 23, 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.	[15.1] The method of claim 13, wherein the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack.	[25.1] The computer system of claim 23, 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 5, wherein the alert further includes predictive information.	[16.1] The method of claim 13, wherein the alert further includes predictive information.		

U.S. Pat. No. 12,231,426 (Claims 1-30)

Claims 1-8	Claims 9-18	Claims 19-25	Claims 26-30
	[17.1] The method of claim 12, further comprising:		
	[17.2] based on the additional verification being required to grant access:		
	[17.3] determining that a probable cyberattack is detected, and		
	[17.4] delivering an alert,		
	[17.5] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and		
	[17.6] wherein the alert is designated to be delivered to an administrator of the network.		
	[18.1] The method of claim 17, wherein the alert further includes predictive information.		