New Rules in Existing Bundles				
Rule ID	Rule Name	Severity	Description	Affected Bundles
D9.AWS.NET.35	Make sure that ALB is protected by a WAF	Medium	Ensure that all your public AWS ALB are integrated with the Web Application Firewall (AWS WAF) service to protect against application-layer attacks	AWS Dome9 Best Practices
D9.AWS.NET.36	AWS CloudFront - WAF Integration	Medium	Ensure that all your AWS CloudFront web distributions are integrated with the Web Application Firewall (AWS WAF) service to protect against application-layer attacks	AWS Dome9 Best Practices
D9.AWS.CRY.15	Use KMS CMK customer-managed keys for Redshift clusters	High	Use customer-managed KMS keys instead of AWS-managed keys, to have granular control over encrypting and encrypting data. Encrypt Redshift clusters with a Customer-managed KMS key. This is a recommended best practice.	AWS PCI-DSS 3.2
D9.AWS.NET.AG1.Instance.27017.TCP	Instance with unencrypted Mongo (TCP:27017) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.389.TCP	Instance with unencrypted LDAP (TCP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.7000.TCP	Instance with unencrypted Cassandra Internode Communication (TCP: 7000) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.7199.TCP	Instance with unencrypted Cassandra Monitoring (TCP:7199) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.Instance.9042.TCP	Instance with unencrypted Cassandra Client (TCP:9042) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.9160.TCP	Instance with unencrypted Cassandra Thrift (TCP:9160) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.6379.TCP	Instance with unencrypted Redis (TCP:6379) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.61620.TCP	Instance with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.8888.TCP	Instance with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.2483.TCP	Instance with unencrypted Oracle DB (TCP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.1521.TCP	Instance with unencrypted Oracle DB (TCP:1521) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.Instance.9200.TCP	Instance with unencrypted Elastic search (TCP:9200) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.9300.TCP	Instance with unencrypted Elastic search (TCP:9300) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.11211.TCP	Instance with unencrypted Memcached (TCP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.389.UDP	Instance with unencrypted LDAP (UDP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.2483.UDP	Instance with unencrypted Oracle DB (UDP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.11211.UDP	Instance with unencrypted Memcached (UDP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.27017.TCP	ELB with unencrypted Mongo (TCP:27017) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ELB.389.TCP	ELB with unencrypted LDAP (TCP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.7000.TCP	ELB with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.7199.TCP	ELB with unencrypted Cassandra Monitoring (TCP:7199) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9042.TCP	ELB with unencrypted Cassandra Client (TCP:9042) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9160.TCP	ELB with unencrypted Cassandra Thrift (TCP:9160) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.6379.TCP	ELB with unencrypted Redis (TCP:6379) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.61620.TCP	ELB with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ELB.8888.TCP	ELB with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.2483.TCP	ELB with unencrypted Oracle DB (TCP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.1521.TCP	ELB with unencrypted Oracle DB (TCP:1521) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9200.TCP	ELB with unencrypted Elastic search (TCP:9200) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9300.TCP	ELB with unencrypted Elastic search (TCP:9300) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.11211.TCP	ELB with unencrypted Memcached (TCP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.389.UDP	ELB with unencrypted LDAP (UDP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ELB.2483.UDP	ELB with unencrypted Oracle DB (UDP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.11211.UDP	ELB with unencrypted Memcached (UDP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.27017.TCP	NetworkLoadBalancer with unencrypted Mongo (TCP:27017) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.389.TCP	NetworkLoadBalancer with unencrypted LDAP (TCP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.7000.TCP	NetworkLoadBalancer with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.7199.TCP	NetworkLoadBalancer with unencrypted Cassandra Monitoring (TCP:7199) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.9042.TCP	NetworkLoadBalancer with unencrypted Cassandra Client (TCP:9042) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.NetworkLoadBalancer.9160.TCP	NetworkLoadBalancer with unencrypted Cassandra Thrift (TCP:9160) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.6379.TCP	NetworkLoadBalancer with unencrypted Redis (TCP:6379) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.61620.TCP	NetworkLoadBalancer with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.8888.TCP	NetworkLoadBalancer with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.2483.TCP	NetworkLoadBalancer with unencrypted Oracle DB (TCP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.1521.TCP	NetworkLoadBalancer with unencrypted Oracle DB (TCP:1521) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.9200.TCP	NetworkLoadBalancer with unencrypted Elastic search (TCP:9200) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.NetworkLoadBalancer.9300.TCP	NetworkLoadBalancer with unencrypted Elastic search (TCP:9300) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.11211.TCP	NetworkLoadBalancer with unencrypted Memcached (TCP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.389.UDP	NetworkLoadBalancer with unencrypted LDAP (UDP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.2483.UDP	NetworkLoadBalancer with unencrypted Oracle DB (UDP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.NetworkLoadBalancer.11211.UDP	NetworkLoadBalancer with unencrypted Memcached (UDP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.27017.TCP	ApplicationLoadBalancer with unencrypted Mongo (TCP:27017) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.389.TCP	ApplicationLoadBalancer with unencrypted LDAP (TCP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ApplicationLoadBalancer.7000.TCP	ApplicationLoadBalancer with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.7199.TCP	ApplicationLoadBalancer with unencrypted Cassandra Monitoring (TCP:7199) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.9042.TCP	ApplicationLoadBalancer with unencrypted Cassandra Client (TCP:9042) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.9160.TCP	ApplicationLoadBalancer with unencrypted Cassandra Thrift (TCP:9160) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.6379.TCP	ApplicationLoadBalancer with unencrypted Redis (TCP:6379) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.61620.TCP	ApplicationLoadBalancer with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.8888.TCP	ApplicationLoadBalancer with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ApplicationLoadBalancer.2483.TCP	ApplicationLoadBalancer with unencrypted Oracle DB (TCP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.1521.TCP	ApplicationLoadBalancer with unencrypted Oracle DB (TCP:1521) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.9200.TCP	ApplicationLoadBalancer with unencrypted Elastic search (TCP:9200) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.9300.TCP	ApplicationLoadBalancer with unencrypted Elastic search (TCP:9300) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.11211.TCP	ApplicationLoadBalancer with unencrypted Memcached (TCP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.389.UDP	ApplicationLoadBalancer with unencrypted LDAP (UDP:389) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ApplicationLoadBalancer.2483.UDP	ApplicationLoadBalancer with unencrypted Oracle DB (UDP:2483) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG1.ApplicationLoadBalancer.11211.UDP	ApplicationLoadBalancer with unencrypted Memcached (UDP:11211) is exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.Instance.22.TCP	Instance with administrative service: SSH (TCP:22) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.Instance.3389.TCP	Instance with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.Instance.9090.TCP	Instance with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ELB.22.TCP	ELB with administrative service: SSH (TCP:22) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ELB.3389.TCP	ELB with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ELB.9090.TCP	ELB with administrative service: CiscoSecure, websm (TCP:9090) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1

D9.AWS.NET.AG4.NetworkLoadBalancer.22.TCP	NetworkLoadBalancer with administrative service: SSH (TCP:22) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.NetworkLoadBalancer.3389.TCP	NetworkLoadBalancer with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.NetworkLoadBalancer.9090.TCP	NetworkLoadBalancer with administrative service: CiscoSecure, websm (TCP:9090) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ApplicationLoadBalancer.22.TCP	ApplicationLoadBalancer with administrative service: SSH (TCP:22) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ApplicationLoadBalancer.3389.TCP	ApplicationLoadBalancer with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.AWS.NET.AG4.ApplicationLoadBalancer.9090.TCP	ApplicationLoadBalancer with administrative service: CiscoSecure, websm (TCP:9090) is too exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	AWS CSA CCM v.3.0.1
D9.GCP.CRY.01	Ensure VM disks are encrypted with Customer-Supplied Encryption Keys (CSEK)	High	By default, GCP encrypts all data with GCP owned keys. You should provide your own encryption keys to manage the Customer-Supplied encryption keys.	GCP ISO 27001:2013
Changes to existing Rules				

Rule ID	Rule Name	Severity	Description	Updated Fields
D9.GCP.NET.09	Ensure that Cloud Storage bucket is not anonymously and/or publicly accessible	High	It is recommended that IAM policy on Cloud Storage bucket does not allows anonymous and/or public access.	logic
D9.AZU.CRY.04	Ensure that the expiry date is set on all SQL Server keys	High	It is recommended that you rotate SQL Server keys in the Azure Key Vault, and set an explicit expiry time for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes. Use Azure Key Vaults to store and use cryptographic keys within the Microsoft Azure environment. The exp (expiration time) attribute identifies the expiration time on or after which the key cannot be used for a cryptographic operation. By default, keys never expire.	name description logic
D9.AZU.NET.06	Remove unused Network Security Groups	Medium	Delete all Network Security Groups which are not in use.	name description logic
D9.AZU.NET.07	Ensure that at least one Network Security Group is attached to all VMs and subnets that are public	High	Attach a Network Security Group to each VM or subnet containing a VM. If no Network Security Group is attached to either the Virtual Machine or the subnet, the VM is not protected and can be accessed from the internet.	name description logic
D9.AWS.CRY.02	ELB is setup with SSL for secure communication	High	Ensure that ELB is configured with SSL, for secure communication. Covers standards HTTPS and AWS Proxy Protocol Config; see https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/using-elb-listenerconfig-quickref.html	logic
D9.GCP.NET.AG - all the port based rules				complianceTag changed to Network Ports Security for all the autogenerated rules
D9.AZU.NET.08	Ensure there is an up to date Network Diagram for your cloud network	Medium	Dome9 Clarity allows you to visualize your Azure Network Security configurations in real time.	name description
D9.GCP.NET.02	Asset is not labeled	Medium	A label is a key-value pair that helps you organize your Google Cloud Platform resources, such as instances. You can attach a label to each resource, then filter the resources based on their labels. Common use for labels: Team or cost center labels Component labels Environment or stage labels Owner or contact labels State labels Virtual machine labels	complianceTag
D9.GCP.NET.05	Ensure there is an up to date Network Diagram for your cloud network	Medium	Dome9 Clarity allows you to visualize your Google Cloud Network Security configurations in real time.	name description
D9.GCP.LOG.01	Ensure that Cloud Storage bucket has logging enabled	High	Turn on logging on all of your Storage Buckets so that you can make sure that all changes are logged and trackable.	name

D9.AZU.CRY.03	Ensure that the expiry date is set on all SQL Database keys	Medium	It is recommended that you rotate SQL Database keys in the Azure Key Vault, and set an explicit expiry time for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes. Use Azure Key Vaults to store and use cryptographic keys within the Microsoft Azure environment. The exp (expiration time) attribute identifies the expiration time on or after which the key cannot be used for a cryptographic operation. By default, keys never expire.	name description
D9.AZU.CRY.05	Ensure that the Redis Cache accepts only SSL connections	High	It is recommended that Redis Cache should allow only SSL connections. Note: some Redis tools (like redis-cli) do not support SSL. When using such tools plain connection ports should be enabled.	name description
D9.AZU.CRY.06	Ensure that 'Secure transfer required' is enabled for Storage Accounts	High	Enable secure transfer (encryption) connections. The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPs. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When you use the Azure files service, connections without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Azure storage does not support HTTPS for custom domain names, so this option is not applied when using a custom domain name.	name description
D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service	High	Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	name description
D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service	High	Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	name
D9.AZU.CRY.11	Ensure that 'Data encryption' is set to 'On' for Azure SQL Database	High	Encrypt SQL Databases. Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.	description
D9.AZU.DR.01	Redis cache should have a backup	Medium	Replicate Redis Cache server data to another Redis Cache server using geo replication. This feature is only available for Premium tier Redis Cache. From performance point of view, Microsoft recommends that both Redis Caches (Primary and the linked secondary) reside in the same region.	name description

D9.AZU.DR.02	Ensure Azure SQL Server data replication with Fail Over groups	Medium	SQL Server data should be replicated to avoid loss of unreplicated data.	name
D9.AZU.IAM.01	Set an Azure SQL Server Active Directory Administrator account	Medium	Configure one Azure Active Directory account, either an individual or Network Security Group account, as an administrator. It is not necessary to configure an Azure AD administrator, but an Azure AD administrator must be configured if you want to use Azure AD accounts to connect to SQL Databases.It is recommended to avoid using names like 'admin' or 'administrator', which are targeted in brute force dictionary attacks.	name description
D9.AZU.IAM.02	Set an Azure SQL Server admin account login	Medium	You must designate a Server admin login when you create an Azure SQL server. SQL server creates this account as a login in the master database. Only one such account can exist. This account connects using SQL Server authentication (username and password). It is recommended to avoid using names like 'admin' or 'administrator', which are targeted in brute force dictionary attacks.	name description
D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication	Medium	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	name description
D9.AZU.MON.03	Ensure that 'Threat Detection' is enabled for Azure SQL Database	Medium	Enable threat detection on SQL databases. SQL threat detection adds an additional layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users will receive an alert on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Threat Detection alerts provide details of suspicious activity and recommend actions on how to investigate and mitigate the threat.	description
D9.AZU.MON.05	Ensure that 'Send alerts to' is enabled for Azure SQL Database	Medium	Configure the email address to which alerts will be sent on detection of anomalous activities on SQL databases. This ensures that any detected anomalous activities are reported as soon as possible, making it more likely the potential risk will be mitigated sooner.	description

D9.AZU.MON.06	Ensure that 'Email service and co-administrators' is 'Enabled' for Azure SQL Database	Low	Configure the service and co-administrator email addresses to which alerts will be sent on detection of anomalous activities on SQL databases. This ensures that any detected anomalous activities are reported as soon as possible, making it more likely the potential risk will be mitigated sooner.	description
D9.AZU.NET.09	Ensure that 'Public access level' is set to Private for blob containers	High	Disable anonymous access to blob containers. It is recommended to not provide anonymous access to blob containers unless it is absolutely necessary. You should use shared access signature token for providing controlled and timed access to blob containers. When you permit anonymous, public read access to a container and its blobs in Azure Blob storage, you can grant read-only access to these resources without sharing your account key, and without requiring a shared access signature.	description
D9.AZU.NET.12	Ensure there are no firewall rules allowing unrestricted access to Redis from the Internet	High	Redis Cache should not allow public access. Firewall rules should be configured to allow only private IP addresses.	name description
D9.AZU.CRY.10	Ensure that storage account access keys are periodically regenerated	Medium	Regenerate storage account access keys periodically. When you create a storage account, Azure generates two 512-bit storage access keys, which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure to these keys is undermined.	description
D9.AZU.NET.02	Ensure the Azure SQL Server has access to the entire Azure infrastructure	High	Azure connections must be enabled to allow applications from Azure to connect to your Azure SQL server. When an application from Azure attempts to connect to your database server, the firewall verifies that Azure connections are allowed. A firewall setting with starting and ending address equal to 0.0.0.0 allows these connections. This option configures the firewall to allow all connections from Azure including connections from the subscriptions of other customers. Make to use Firewall VNet rules.	name description
D9.AZU.NET.03	Restrict Azure SQL Server accessibility to a minimal address range	Medium	It is recommended to limit the source IP ranges that are allowed to access the SQL Server, to the minimum necessary.	name description
D9.AZU.NET.11	Ensure there are no firewall rules allowing unrestricted access to Redis from other Azure sources	High	Redis Cache should not be configured to allow unlimited access. If a firewall rule is configured to allow start IP and end IP addresses both from 0.0.0.0/0 then the Redis Cache is open to any Azure source.	name description

D9.AZU.NET.13	Ensure there are no firewall rules allowing Redis Cache access for a large number of source IPs	Medium	It is recommended that the number of source IP addresses that can access the Redis Cache service be restricted. When firewall rules are configured, only allow connections from necessary IP address ranges.	name description
D9.AZU.CRY.01	Ensure that KeyVault is in use	Low	Use the Azure Key Vault to store secrets within the Microsoft Azure environment. Secrets in Azure Key Vault are octet sequences with a maximum size of 25k bytes each.	name description
D9.AZU.CRY.12	Ensure that the expiry date is set on all keys	High	Ensure that all Keys in Azure Key Vault have an expiry time set.	name
D9.AZU.CRY.13	Ensure that the expiry date is set on all secrets	High	Ensure that all Secrets in Azure Key Vault have an expiry time set.	name
D9.AZU.AS.01	Storage Accounts outside Europe	High	Identify Storage Accounts outside of the following regions: northeurope, westeurope	name description
D9.AWS.CRY.05	Use Encrypted RDS storage	High	Encrypt Amazon RDS instances and snapshots at rest, by enabling the encryption option for your Amazon RDS DB instance.	name complianceTag
D9.AWS.CRY.18	DynamoDB data at rest has server side encryption (SSE)	High	Verify that AWS DynamoDB storage at rest is encrypted using Server-Side Encryption (SSE).	name description
D9.AWS.CRY.19	ECS Cluster At-Rest Encryption	High	Ensure that AWS ECS clusters are encrypted. Data encryption at rest, prevents unauthorized users from accessing sensitive data on your AWS ECS clusters and associated cache storage systems.	description
D9.AWS.NET.01	Ensure no security groups allow ingress from 0.0.0.0 /0 to SSH (TCP:22)	High	Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access to port 22.	complianceTag
D9.AWS.NET.02	Ensure no security groups allow ingress from 0.0.0.0 /0 to RDP (TCP:3389)	High	Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access to port 3389.	complianceTag
D9.AWS.NET.04	Ensure the default security group restricts all traffic	High	A VPC comes with a default security group whose initial settings deny all inbound traffic, allow all outbound traffic, and allow all traffic between instances assigned to the security group. If you don't specify a security group when you launch an instance, the instance is automatically assigned to this default security group. Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that the default security group restrict all traffic. Configuring the default security group to restrict all traffic will encourage least privilege security group development and mindful placement of AWS resource into security groups which will in-turn reduce the exposure of those resources.	complianceTag

D9.AWS.NET.06	Ensure S3 buckets are not publicly accessible	High	Misconfigured S3 buckets can leak private information to the entire internet or allow unauthorized data tampering / deletion. Dome9 Clarity intuitively map network traffic sources, security groups, instances, rds, elbs and traffic flow thus facilitating the adherence to maintaining a network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	complianceTag
D9.AWS.NET.07	Ensure there is an up to date Network Diagram for your cloud network	Medium	Dome9 Clarity allows you to visualize your Amazon Network Security configurations in real time.	name complianceTag description
D9.AWS.NET.08	Ensure no security groups allow ingress from 0.0.0.0 /0 to ALL ports and protocols	High	Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access	complianceTag
D9.AWS.NET.09	Restrict outbound traffic to that which is necessary, and specifically deny all other traffic	Medium	Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted egress access	complianceTag
D9.AWS.NET.23	Security Groups - with admin ports too exposed to the public internet	High	Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access to administrative ports ports.	complianceTag
D9.AZU.NET.14	Ensure that Redis is updated regularly with security and operational updates. Note this feature is only available to Premium tier Redis Caches.	High	Enable Azure Redis Cache scheduled updates. This allows security (or operational) updates to be applied, with minimal affect to a running Redis Cache. The default maintenance window for updates is five hours. Note: this feature refers to the Redis Cache server updates and not Azure updates or updates to the operating system of the VMs that host the cache.	name description

Rules Removed

Rule ID	Rule Name	Severity	Description	Affected Bundles
D9.GCP.NET.10	Ensure that there are no publicly accessible objects in storage buckets	High	Allowing public access to objects allows anyone with an internet connection to access sensitive data that is important to your business. IAM is used to control access over an entire bucket however to customize access to individual objects within a bucket ACLs are used. Even if IAM applied on storage does not allow access to "allUsers" there could be object specific ACLs that allows public access to the specific objects inside the bucket. Hence its is important to check ACLs at individual object level.	GCP PCI-DSS 3.2 GCP NIST CSF v1.1 GCP ISO 27001:2013 GCP NIST 800-53 Rev 4 GCP Dome9 Best Practices

D9.AWS.OPE.01	Lambda Functions must have an associated tag	Medium	Tags are key-value pairs that you attach to AWS resources to better organize them. They are particularly useful when you have many resources of the same type, which in the case of AWS Lambda, is a function. By using tags, customers with hundreds of Lambda functions can easily access and analyze a specific set by filtering on those that contain the same tag. Two of the key advantages of tagging your Lambda functions are: Grouping and Filtering and Cost allocation.	AWS Dome9 Best Practices - Sample AWS ISO 27001:2013 AWS Dome9 Best