AWS Support Plan & Trusted Advisor

AWS Account Support Plans:

AWS Account Support Plans:
(1) Basic   Included with any AWS Account
(2) Developer   Starts at $29 per month
(3) Business   Starts at $100 per month
(4) Enterprise   Starts at $15,000 per month

Although you get AWS support with each plan, the basic incentive to purchase a more expensive plan is the speed/availability in which you are given support. Enterprise plan holders will receive the highest priority for access to customer service, and technical support.

For example:
Basic plan holders go no access to a cloud support representative.
Developer plan holders get business hours access to a Cloud Support Associate.
Business plan holders get 24x7 access to a Cloud Support Engineer.
Enterprise plan holders get 24x7 access to a Sr. Cloud Support Engineer.

A full comparison list can be found **here**

As part of all support plans, an AWS Best Practices and Advisory service is included called
AWS Trusted Advisor

What is AWS Trusted Advisor?

Simple Definition:
AWS Trusted Advisor is a service that "advises" and helps you optimize aspects of your AWS account.

AWS Definition:
"An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices."

Trusted Advisor Categories:
(1) Cost Optimization
(2) Performance
(3) Security
(4) Fault Tolerance

AWS Trusted Advisor has different level of support based on the type of AWS _support_ account you have (Basic, Developer, Business, or Enterprise)

Trusted Advisor Services:

Available to all AWS Support Plan Accounts:

Six checks that cover basic security and performance:
(1) Security Groups (port checks)
(2) IAM Use
(3) Is Multi-Factor Authentication (MFA) enabled on the root IAM user account
(4) EBS Public Snapshots
(5) RDS Public Snapshots
(6) Service Limits

Available to Only Business and Enterprise Support Plan Accounts:

(1) Access to full list of Trusted Advisor Checks (full list)
(2) Notifications to stay up-to-date with weekly resource deployments
(3) Programmatic access to retrieve/refresh Trusted Advisor results via API.

With all this talk about support, what should you do if your AWS account becomes compromised?

Is Your Account Compromised?

If your account is (or think it is) compromised - follow these steps:

(1) Change your AWS root account password
(2) Change all IAM user's passwords
(3) Delete or rotate all programmatic (API) access keys
(4) Delete any resources in your account that you did not create

(5) Respond to any notifications you received from AWS through the AWS Support Center and/or Contact AWS Support to open a support case.