WHITE PAPER

# Removing ID

**How to use Vanguard security products to remove ID(*) access greater than NONE or READ to create a more secure mainframe RACF database without risking an operational outage due to removing required access.**

**NOTE: This process is not to be used for Grouping/ Member Classes. Those will be covered in another white paper.**

## The Issue:

Most organizations have no idea who or what processes rely upon the ID (*) permission in order to gain access to a needed resource. Additionally even with AUDIT(ALL) specified on the profile, it is nearly impossible, very time consuming and very CPU intensive to gather 365 days or more worth of SMF data in order to even begin the process of determining who or what process gained access to a resource (including Datasets) via an ID(*) permission.

## The Problem:

With the increased scrutiny by auditors of security on the mainframe and the realization that ID(*) access provides all authenticated users access to resources, the removal of these ID(*) permissions has become a requirement that requires resolution.

## The Solution:

There is one fool proof method to identify and remediate all ID(*) access in a RACF database. Vanguard Administrator and Offline combined with Policy Manager and Enforcer work to maintain the RACF database once remediated. After all, fixing the database only provides relief until someone modifies it and changes the profiles back to an undesirable state.

THE HOW (The technical details of how to resolve this problem)

With the Vanguard Offline and Vanguard Administrator solution, it is possible to determine any and all access to all resource via an ID(*) permission and then remove that access Here is how the process works:

# Removing ID

## First:

You must install the Vanguard CleanUp product and allow it to collect data for a period of time. The length of time depends on the customer installations desire for complete reporting. 365 days is a recommended value but a smaller amount of time can be used as long as end of year processing has been completed.

## Second:

Go into Vanguard Administrator and either against a current Vanguard Extract File or the LIVE database go into option 3: Security Server Reports and then Option 17: ID in Access List. On the next panel specify * in the ID Type: field , this will result in a report of all ID(*) access.. You should do this BY CLASS (No need to try and boil the ocean) so add further Masking below to do one class at a time (such as specifying DATASET on the CLASS Line). Do this ONLINE (so Specify O on the Batch/Online field) as we will use QuickGen to create the commands in the next step, so specify O on the BATCH/One-Line. Generate Heading should be set to N. Now Choose Option 1 on the command line and hit “enter”.

## Third:

Create the commands to change the UACC on all results to NONE. Once the report comes back online, Type QG on the command line and then specify either one of the following on line 1:

For the DATASET CLASS for GENERIC profiles:

PE ‘&PROFILE’ CLASS(&CLASS) ID(*) DELETE GEN For NON DATASET CLASSES PE &PROFILE CLASS(&CLASS) ID(*) DELETE

Then on the command line type : GEN

This will create a temporary file of all the commands you will needs for testing, that you should now copy to a permanent file (call it anything you want, it can be a flat file or a member in a PDS, but remember the name of this file). This file will be later in this document as the COMMANDFILE.

**NOTE: DO NOT ISSUE the VRAEXEC, VRABATCH or VRASCHED command or in any way submit this set of commands to your RACF database as: YOU DO NOT WANT to remove access yet. DON’T DO IT.**

## Fourth:

Now that we have removed ID(*) to NONE, we need to find out what the effect of the commands will have given actual accesses (those captured by the Vanguard CleanUp Started task from the First Step) that occurred to the production RACF database so that we can find what users will lose access, given the changes.

What we do here in Targeted Impact Analysis Option 4 is take every access Request from that Offline HMF that could be affected by the Commands in the COMMANDFILE and test them against the Test RACF database (the Offline version) and store the results (no we don't use RACF to do this, it is all Vanguard Processing) and then we execute the Commands in the COMMANDFILE against the Test RACF database (the Offline version) and then rerun the same set of Access Requests against the now modified test RACF database (now having the effect of the COMMANDFILE run against it) and then we compare the two resultant sets of ACCESS. Any difference found is directly due to the effect of the commands in the COMMANDFILE and ONLY those commands.

To accomplish this go into Vanguard Offline, Specifying Option 7 for Targeted Impact Analysis reports and then chose Option 4. On the Option 4 screen , you will need to provide the COMMANDFILE name on the Command Input Dataset Line and you will specify the name of the offline copy of the RACF database (Option 4, will delete , define and create the copy at run time of the RACF database based on the system it executes upon). The History Master File is determined based on the VCLOPT00 and MUST point to your production Offline History Master File (This can be found in VCLOPT00 specified as VOFMAST).

Next , On the Targeted Impact Analysis Screen you will see a CREATE EXTRACT FILE option, please specify this as YES, provide it a meaningful name as this flat file dataset will be used later. This file will be referred to as RESULTSET later in this white paper.

Hit Enter to get to the next screen which allows for specification of one or more Offline HMFs. if you are running Offline on multiple systems against different Offline HMFs within a sysplex against the same RACF database, you should specify the names of the other HMFs here.

Hit Enter and then submit the generated JCL after making any necessary JOBCARD modifications. The job may run awhile depending on the size of the RACF database and more importantly the number of access requested contained in the Vanguard Offline History Master File.

## Fifth:

Now it is time to see the effect of the COMMANDFILE and generate permits for users that would lose access due to their use of the UACC to gain access to resources. Once the batch file from the previous step is completed, Go back into Vanguard Offline and chose Option 6: Target Impact Analysis Report Online (the file created in the step above should now show on the Extract File line) and then option 7 Impact Detail – All Access Changes (which if you only issued commands that will lower ID(*) access, then all records reflected will be denied access as lowering a ID(*)access cannot provide additional Access).

On the command line put a Q for QUICKGEN and on line 1: Type one of the following:
For the generic profile datasets: **PE ‘&AUTHPROF’ CLASS(&CLASS) ID(&USERID) ACCESS (&LACCREQ) GEN**

For General Resource class members: **PE &AUTHPROF CLASS(&CLASS) ID(&USERID) ACCESS (&LACCREQ)**

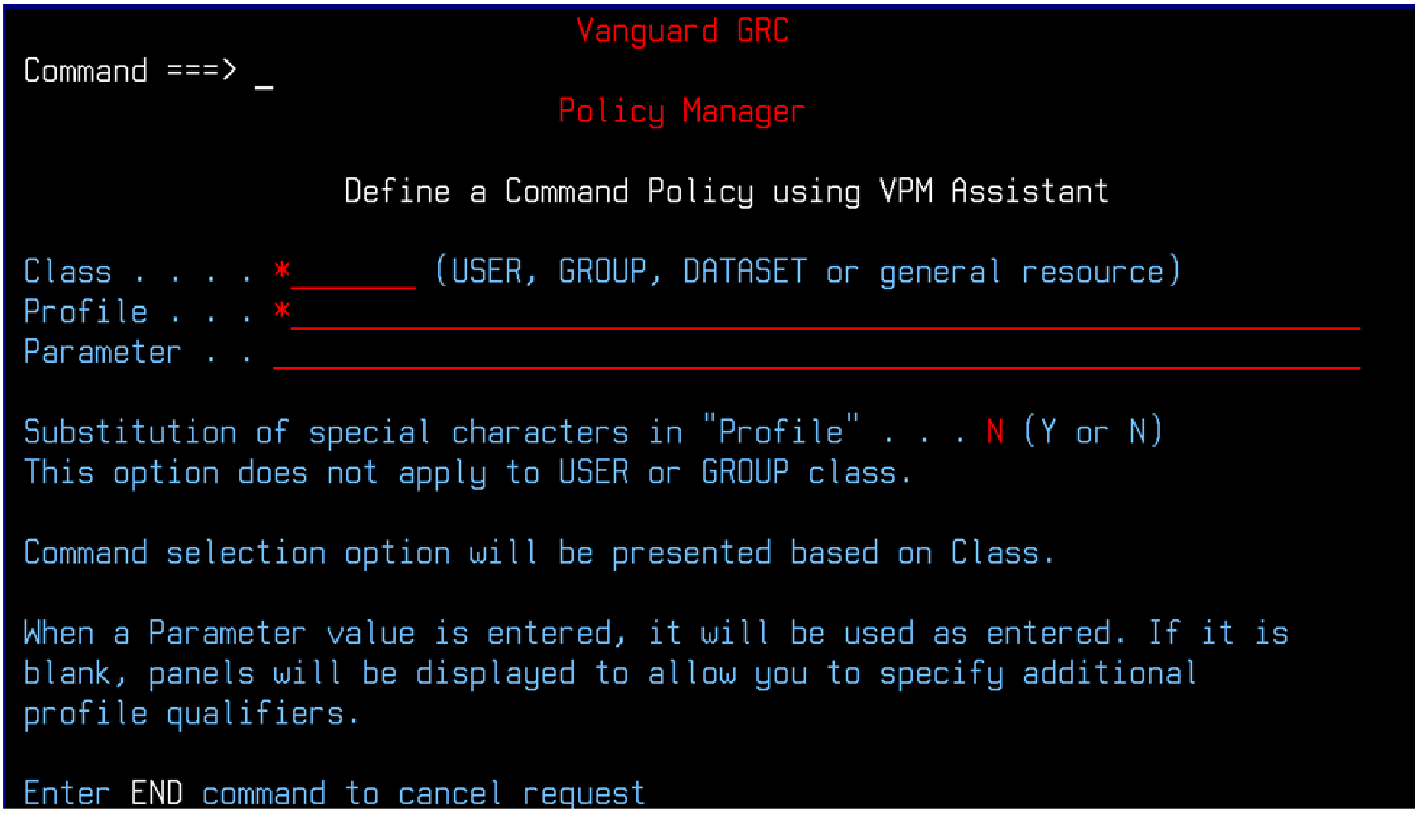
Take the resultant set of commands and save them as a new set of commands, this will be referred to as the PERMITUSERID below.

LAST:
Now, once you are ready to actually remediate your RACF database by setting the ID(*) to NONE, take the PERMITUSERID commands and the COMMANDFILE and run them against your RACF database back to back running the PERMITUSERID first. You can do this in a batch job or online.

TO PREVENT ID(*) above NONE being changed in the future.

Vanguard Policy Manager should be implemented on the target system to prevent undesirable changes from being reintroduced back into the RACF database by well-intentioned Administrators. Install Policy Manager on the system and then implement the following Policy.

*.PERMIT.*.ID.IDASTERISK



```
                              Vanguard GRC
Command ===> _
                             Policy Manager

                 Define a Command Policy using VPM Assistant

Class . . . . *_______ (USER, GROUP, DATASET or general resource)
Profile . . . *____________________________________________________________
Parameter . . _____________________________________________________________

Substitution of special characters in "Profile" . . . N (Y or N)
This option does not apply to USER or GROUP class.

Command selection option will be presented based on Class.

When a Parameter value is entered, it will be used as entered. If it is
blank, panels will be displayed to allow you to specify additional
profile qualifiers.

Enter END command to cancel request
```

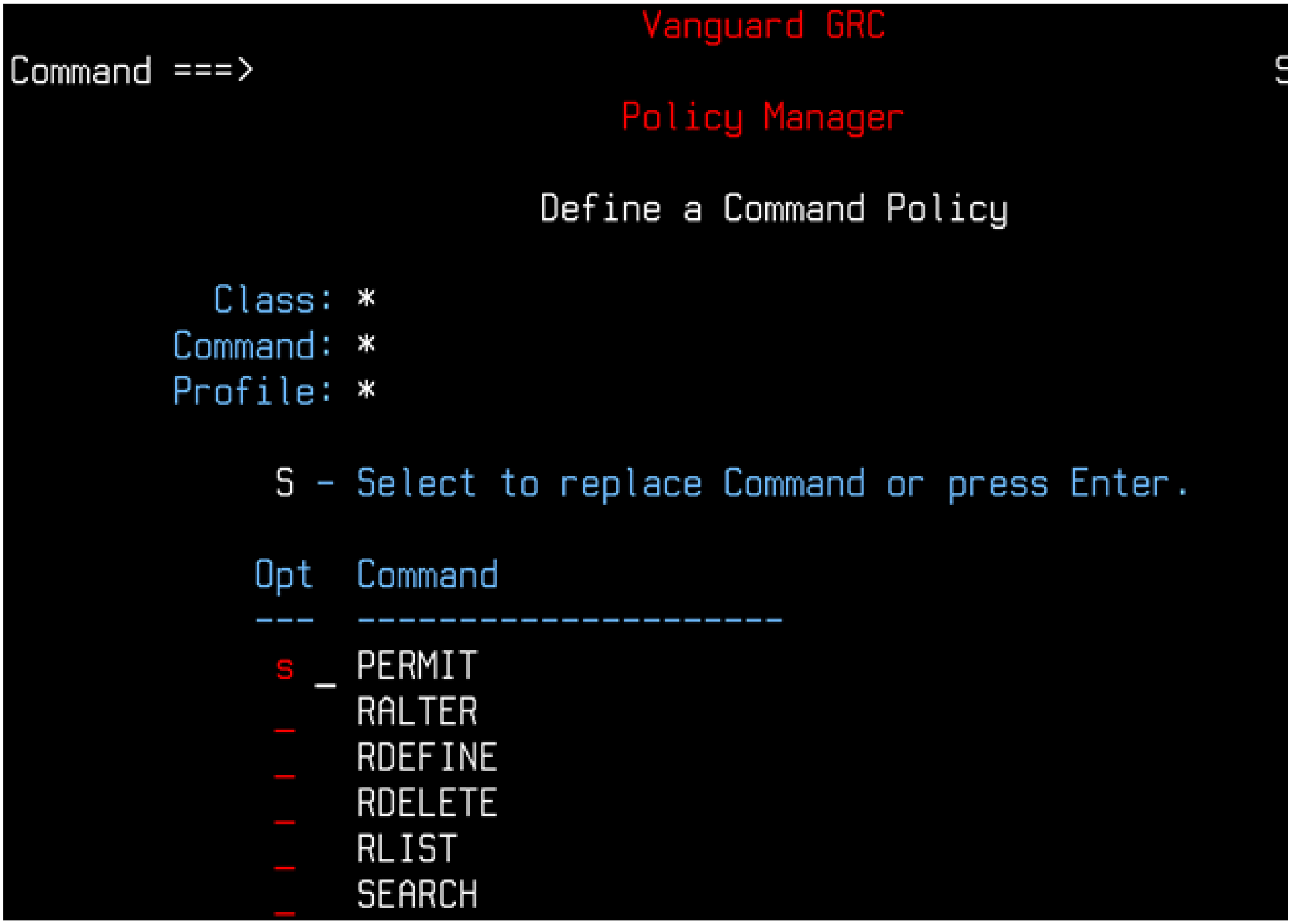
# Removing ID

Go into option 2 command policies

Option 3 Define a command policy using VPM Assistant.

Substitution of special characters in "Profile" . . . N This must be NO, otherwise the profile will not be correct in the last step when you type DEF to define it later.

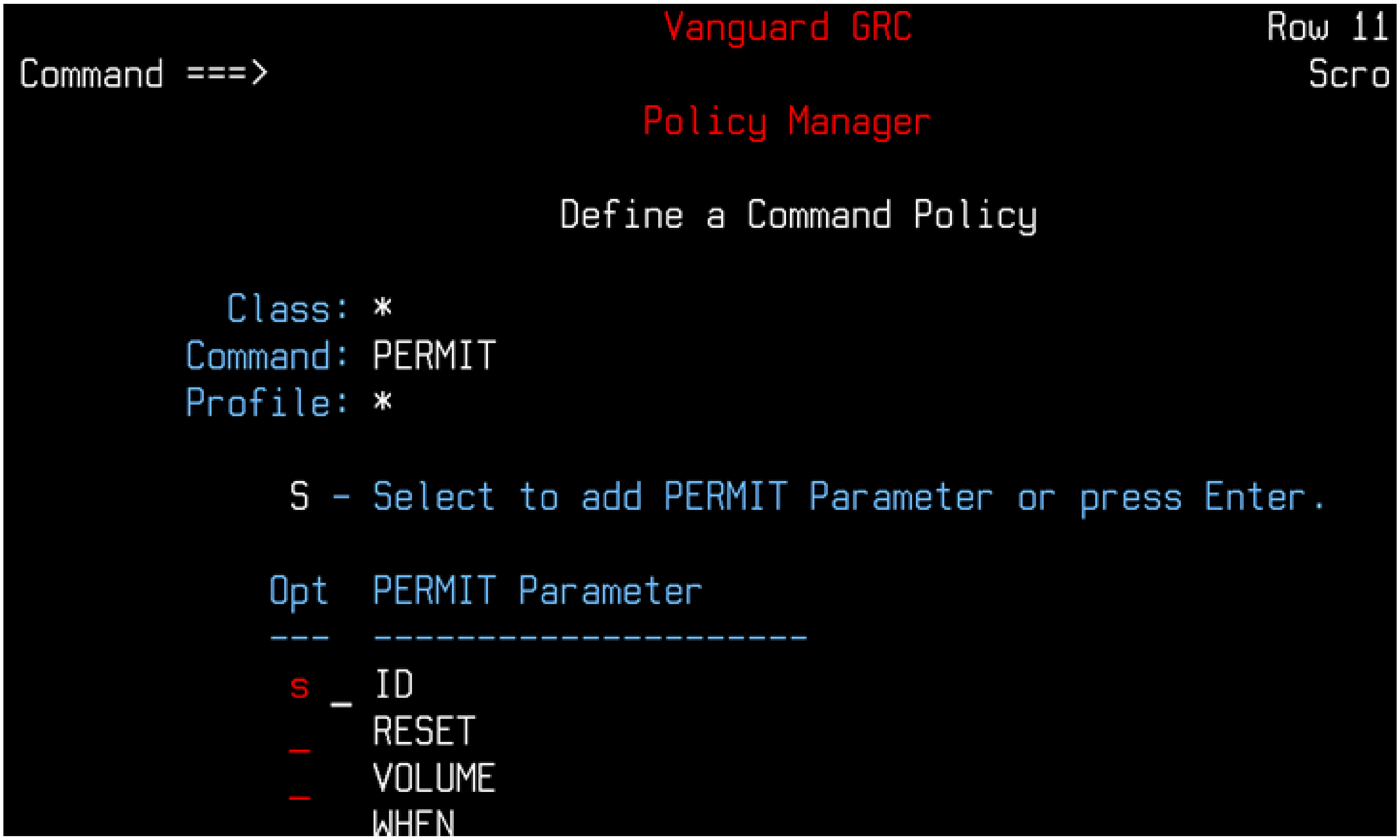
Hit Enter Choose PERMIT on the next panel by selecting it.



```
                               Vanguard GRC
Command ===>                                                          S
                              Policy Manager

                           Define a Command Policy

          Class: *
        Command: *
        Profile: *

             S - Select to replace Command or press Enter.

               Opt  Command
               ---  ---------------------
               s _  PERMIT
               _    RALTER
               _    RDEFINE
               _    RDELETE
               _    RLIST
               _    SEARCH
```

# Removing ID

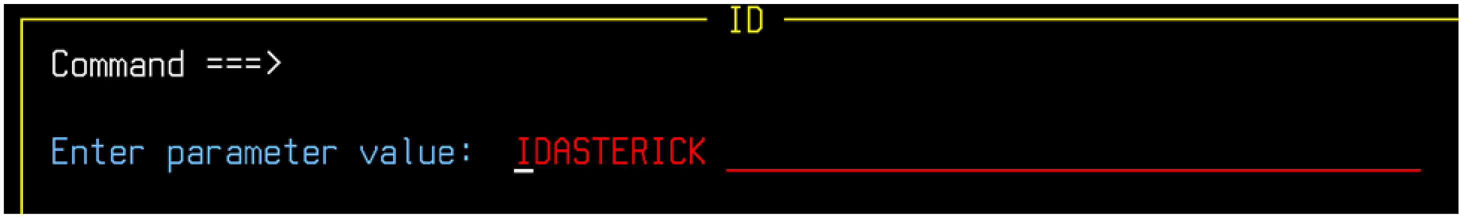
Hit Enter: Select ID on next panel, you may need to page down depending on how large the window size to get to it:



```
                              Vanguard GRC                          Row 11
Command ===>                                                          Scro
                             Policy Manager

                         Define a Command Policy

         Class: *
       Command: PERMIT
       Profile: *

              S - Select to add PERMIT Parameter or press Enter.

              Opt  PERMIT Parameter
              ---  ---------------------
              s _  ID
              _    RESET
              _    VOLUME
                   WHEN
```

Hit Enter:

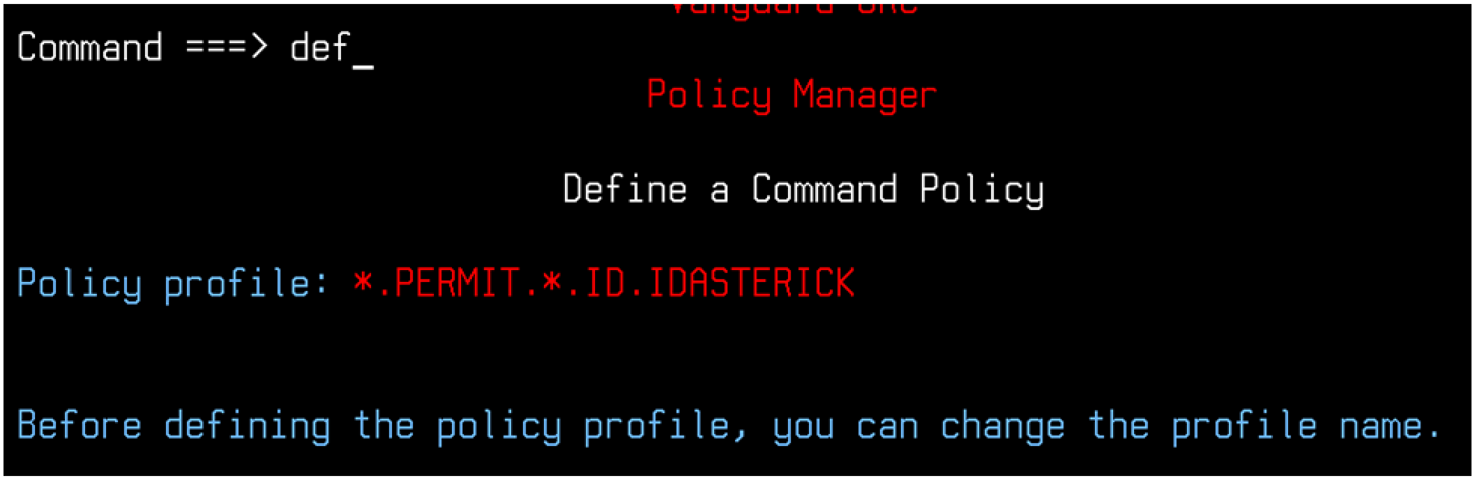
On popup type IDASTERICK



```
                                  ID
  Command ===>

  Enter parameter value:  IDASTERICK
```

Hit Enter:

On the next panel type DEF on the next panel command line after you validate that the profile looks like it does below and then hit enter again.



```
                              Vanguard One
Command ===> def_
                                Policy Manager

                            Define a Command Policy

Policy profile: *.PERMIT.*.ID.IDASTERICK


Before defining the policy profile, you can change the profile name.
```

*.PERMIT.*.ID.IDASTERISK The profile should look exactly like this.

If it looks like this:
*.PERMIT.+.ID.IDASTERISK then you did not specify N on Substitution of special characters in "Profile". Please go back to that step by hitting F3 until you get to it and try again.

Vanguard Policy Manager creates the command profile and assuming Policy Manager has been activated on this system, Policy Manager will immediately start enforcing the policy.

## Why Vanguard to Secure Your Enterprise?

Almost half of the Fortune 1000 companies in the world spanning banking, retail, insurance, as well as numerous government agencies trust Vanguard with their enterprise security.

## About Vanguard Security Solutions

Vanguard offers the most advanced and integrated portfolio of enterprise security products and services in the world. The portfolio was the first to offer fully automated baseline configuration scanner for Mainframe DISA STIGs— the Gold Standard for Security.

## For More Information

To learn more about Vanguard Security Solutions please
call 702.794.0014 or visit www.go2vanguard.com

## Corporate Headquarters

6625 S. Eastern Avenue—Suite 100
Las Vegas, NV 89119-3930