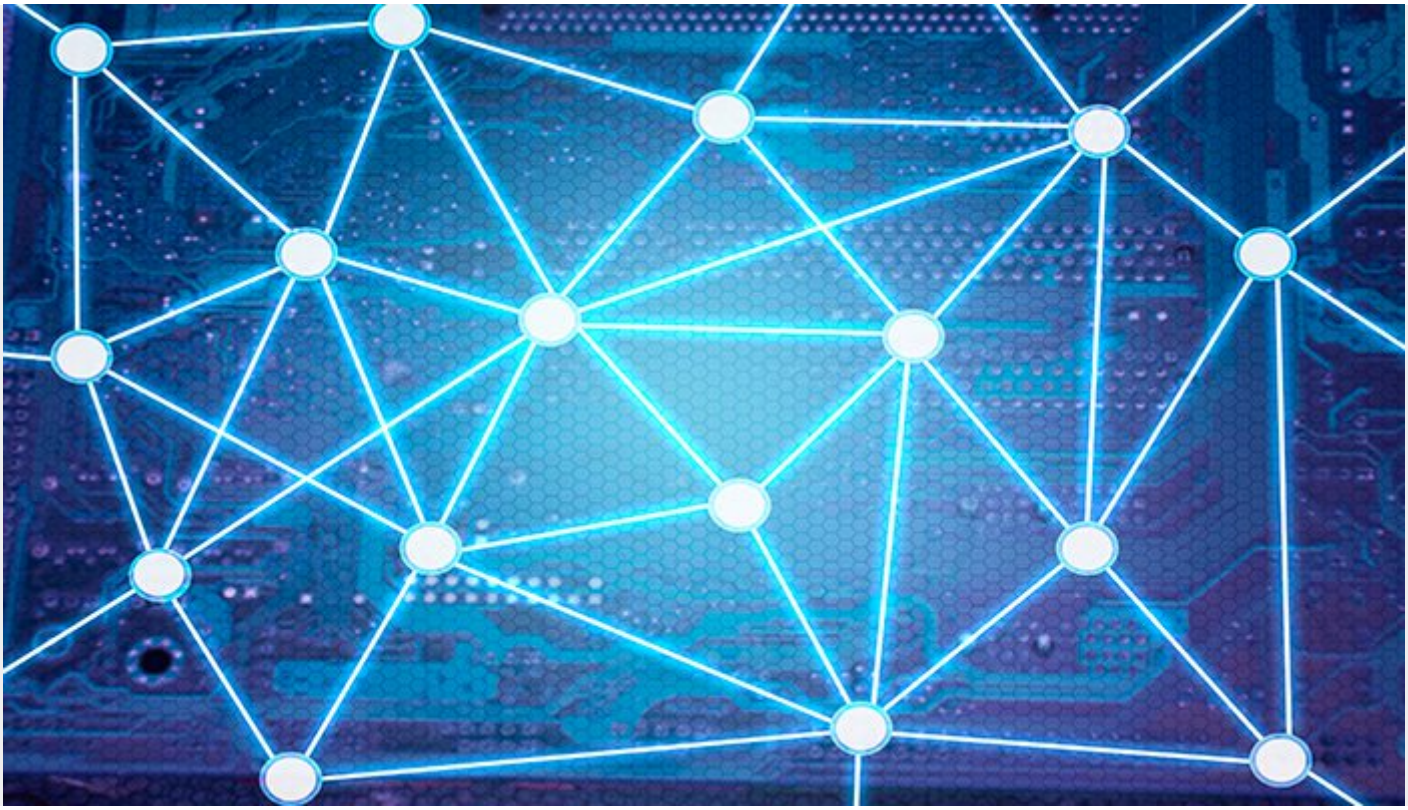
TEST DRIVE SELF-DRIVING REMEDIATION



If you haven't already taken Self-Driving Remediation (a new feature of TrueSight Cloud Security) for a test drive, then you probably are wondering what it means for you and your cloud security posture management. Let me clarify before discussing why one should use it.

You know the difference between a car and a self-driving car. In the former, you drive the car, making numerous, seemingly instinctive decisions as you manoeuvre through traffic. In contrast, in self-driving mode – admittedly something most of us do not have a lot of personal experience with – probably all you need to do is tell the car the destination and then just sit back and relax, perhaps using your commute time for higher value activity than just moving from Point A to B. With TrueSight Cloud Security, On-Demand Remediation and Self-Driving Remediation operate in similar fashion.

Difference between On-Demand Remediation and Self-Driving Remediation

As a cloud operations member or an application developer, one of your primary tasks is to ensure that the configurations of all cloud resources are consistent with security standards. Depending upon how frequently you make changes to your cloud resources, you would login to TrueSight Cloud Security (TSCS) and look for any violations reported for the resources which you own. Then you go through each violation, look at the resources which have violated a specific rule, and then click the "Remediate Violations" button. This is On-Demand Remediation, an **automated** means of fixing cloud resource misconfigurations with a simple click of the mouse.

As our Cloud SecOps processes mature, we may become increasingly comfortable with remediating certain violations, under certain conditions, without any human intervention. For non-production environments like DEV, TEST, or STAGE, we may even have a zero-tolerance policy for any violation and would like to remediate all violations immediately as soon as they are reported. This fully **automatic** remediation gives a powerful mechanism to ensure that configuration security is assured and that any exceptions are documented, added to "Exceptions" in TSCS, and approved for production. To enable Self-Driving Remediation in TSCS, simply set the remediation trigger "Auto" for specific policies. In this case the remediation is automatically triggered when the violation is identified, thereby eliminating the human bottleneck and rapidly closing vulnerabilities from cloud resource misconfigurations.

Why Use Self-Driving Remediation?

First, it saves lot of time going through each known violation and clicking the Remediate Violation button. Although automated, such repetitive tasks, while comforting in that they offer a sense of control, are begging to be handed over to the solution for completely automatic handling. For example, if you know a specific violation must be remediated every time it is identified in certain cloud accounts, just enable the "Auto" remediation trigger from the violation page. The time you save can be spent elsewhere.

Secondly, Self-Driving Remediation helps enforce certain security practices without fail. You don't have to wait for someone to log into TSCS to identify the violations and initiate remediation, or wait for someone to act on a compliance summary or new violation notification email. As an enterprise, if you don't want any S3 bucket to be publicly accessible, then simply go to the Manage Policy page and set the remediation trigger to "Auto" for that rule. Anytime a violation is reported for that rule, remediation will be initiated then and there. Doesn't that bring you more peace of mind?

Next, if you worry that you may not want to perform same remedial action for all accounts, and for some you want a separate action to be invoked, you can do that too. You can configure one remedial action for a certain group of accounts and another remedial action for another group of accounts. You can even create your custom actions.

Finally, if you fear that you may not be aware of all the remediations that are happening, or you want an approval process to kick in for certain resources before they are acted upon, then let me assure you that you can **enable change management** for remediation. In so doing, you will have a formal change approval process for your most critical applications.

In summary, you are still in control. You decide the conditions in which Self-Driving Remediation takes the wheel. So, take the plunge now and see for yourself if it saves your time and helps you concentrate on more challenging things and make your time count!