BitLocker and TPM Status Dashboard

With Endpoint Insights' **BitLocker and TPM Status** dashboard you can quickly see the number of computers that are completely protected. In addition, you can see how many computers either need BitLocker enabled or have a TPM issue.

Here's a breakdown of each state by color:

Green = Protected

Yellow = BitLocker is Not Enabled on All Drives

Orange = BitLocker is Turned Off

Pink = BitLocker is Not Enabled

Red = TPM Issue

Protected means that the system is fully encrypted with BitLocker and TPM is correct.

BitLocker is Not Enabled on All Drives means that TPM is setup and ready to use, but a computer has more than one drive within the system where at least one of the drives is not encrypted with BitLocker. Generally the solution is to enable BitLocker on all drives.

BitLocker is Turned Off means that TPM is setup and ready to use, but BitLocker is not turned on. The solution is to turn on BitLocker on all drives.

BitLocker is Not Enabled means that TPM is setup and ready to use and BitLocker is configured to be used, but as may be the case with servers, the BitLocker feature might not be installed (enabled). The solution is to install and configure BitLocker on all drives.

TPM Issue means TPM is either not installed on the computer or it is not enabled within the BIOS. The solution varies depending on the problem, but in some cases it could mean a hardware upgrade, i.e. replacing old computers with ones where TPM is installed.

As mentioned earlier, this dashboard leverages the inventory information of both TPM's and BitLocker's state from SCCM current branch.