

17. Monitore logs de DHCP para dispositivos conectados

Você deve saber o que está conectado à sua rede. Se possui vários locais com muitos usuários e computadores, isso pode ser um grande desafio.

Existem maneiras de evitar que apenas dispositivos autorizados se conectem, mas isso pode ser caro e muito trabalhoso para configurar. Se você tem os recursos (\$\$\$\$), esse é o caminho a percorrer.

Outro método que já está disponível para você é monitorar os logs de DHCP dos dispositivos conectados.

Você deve ter todos os dispositivos de usuário final configurados para usar o DHCP. Com isso pode então olhar os logs para ver o que está conectando. Você deve ter uma convenção de nomenclatura para o seu equipamento, isso tornará mais fácil identificar possíveis dispositivos não autorizados.

Dispositivos desconhecidos devem ser investigados.