ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE TRANSPORTE E OBRAS PÚBLICAS

Núcleo de Teconologia da Informação e Comunicação

Parecer Técnico nº 1/SETOP/NTIC/2018

PROCESSO Nº 1300.01.0000223/2018-27

PARECER CONCLUSIVO - Edital PE 1301017 000049/2018

Tendo em vista o prazo concedido para apresentação de NOVA DOCUMENTAÇÃO para análise quanto ao atendimento das características técnicas do objeto licitado, e com fulcro no disposto do § 3º do art. 48 da Lei Federal nº 8.666/93, consideramos que as justificativas apresentadas no documento "*QUESTIONAMENTOS - Respostas.pdf*" apresentado pela Licitante para os itens descritos abaixo, não atendem as exigências do edital, tornando INABILITADA a empresa BRINFOR SOLUÇÕES EM TI LTDA-ME que apresentou a proposta de melhor preço, por desatendimento das exigências das características técnicas previstas no edital, conforme razões apresentadas nos respectivos itens pela área técnica do Núcleo de Tecnologia da Informação e Comunicação da SETOP.

1.3. A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas as fermentas para a monitoração e controle da proteção dos dispositivos:

Conforme o manual, a Bitdefender não consegue cumprir com todas as funcionalidades exigidas no edital, somente com a console em nuvem.

1.7. Deve permitir sincronização com o Active Directory (AD), para gestão de usuários e grupos integrados às políticas de proteção:

Conforme o manual, a Bitdefender só atende a esse item com a instalação da sua console de gerência em virtual APPLIANCE, ou seja, localmente. Não cumprem o item 1.3 onde é informado que toda a configuração e a console de gerência deve ser hospedada em nuvem, e não localmente.

1.10. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando:

Não encontrado no manual a referência que possibilite a proteção por usuário e não por dispositivo.

1.13. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs:

Conforme o manual, a comprovação enviada se refere a permissão do usuário modificar regras no agente instalado no ENDPOINT. Não faz nenhuma referência de criação de níveis de acesso a CONSOLE. A Bitdefender não possui essa funcionalidade.

1.48.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo):

Não está claro a existência de ACL's. Todos os dados a serem protegidos devem ser inseridos manualmente.

1.48.3. Possibilitar o bloqueio, somente registrar o evento na Console de Administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível:

Na documentação menciona um controle sobre dispositivo e não uma comprovação de DLP para transferência de dados pendriveis, seja ela em pendrive ou por e-mail como a funcionalidade exige.

1.48.4. Deve possuir listas de CCLs pré-configuradas com no mínimo as seguintes identificações:

1.48.4.1. Números de cartões de crédito;

1.48.4.2. Números de contas bancárias;

1.48.4.3. Números de Passaportes;

1.48.4.4. Endereços;

1.48.4.5. Números de telefone;

1.48.4.6. Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;

1.48.4.7. Lista de e-mails;

O edital informa que deve existir listas de CCLs pré-configuradas. O que é informado na documentação é a criação MANUALMENTE de listas de conteúdos, o que não atende ao edital.

1.48.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade:

Não encontrado no manual a referência da criação da regra através de um assistente de criação da regra. A Bitdefender não possui essa funcionalidade.

1.48.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo:

O item pede a proteção para prevenção de perda de dados e não controle dos dispositivos, o que se entende que a Bitdefender não consegue atender ao exigido no edital.

1.48.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação:

No manual, não menciona que a Bitdefender consegue registrar a movimentação de dados sensíveis e registrar em relatório. O mostrado na comprovação enviada não informa o procedimento e nem o atendimento.

Funcionalidades não encontradas:

1.49.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas:

MALWARE e EXPLOITS tem ações distintas. A exploração de vulnerabilidade se dá em busca de falhas em aplicações e sistemas operacionais para se obter acessos administrativos a máquina e DEPOIS instalar um malware. Na documentação enviada, não demonstra que a Bitdefender consegue atender esse item.

3.2.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus:

A documentação enviada não está clara quanto a capacidade de detectar vírus em Macros.

Belo Horizonte, 10 de outubro de 2018.

Ricardo Miranda

Pregoeiro

Documento assinado eletronicamente por **Ricardo Luiz Miranda**, **Chefe do Núcleo**, em 10/10/2018, às 11:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1987772** e o código CRC **98994215**.

Referência: Processo nº 1300.01.0000223/2018-27 SEI nº 1987772