DECISÃO DE DESCLASSIFICAÇÃO

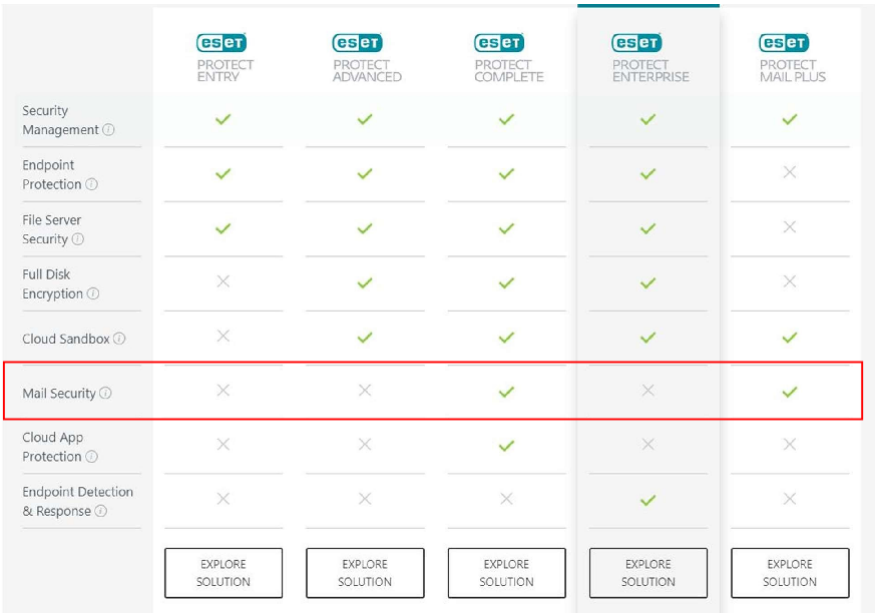
Trata-se este de um procedimento licitatório, na modalidade Pregão Eletrônico de n° 119/2021, cujo o objeto é o Registro de Preços para contratação de soluções de segurança do tipo endpoint protection (antivírus) e de gateway de e-mail (AntiSpam), incluindo serviços de instalação, console de gerenciamento, suporte técnico on site, garantia e atualização por 36 (trinta e seis) meses.

No dia 01/10/2021 a documentações técnicas da empresa **BRINFOR SOLUÇÕES EM TI LTDA** foram encaminhadas para análise e manifestação do setor técnico da Secretaria Municipal de Tecnologia e Inovação, o qual emitiu o seguinte parecer:

> Vieram os autos a esta subsecretaria para fins de análise e parecer acerca dos aspectos técnicos, proposta comercial e demais exigência do Termo de Referência, conforme se observa do despacho de evento nº 33.
>
> Após análise detida da documentação encaminhada pela empresa BRINFOR SOLUÇÕES EM TI LTDA, atual arrematante do certame, verificamos que a solução proposta não atende às seguintes exigências/requisitos do Termo de Referência:
>
> **Soluções da ESET que foram ofertadas:**

Item	Descrição do Objeto	Marca/Modelo	Und.	Qt.	Pr.Unit.	Pr. Total
01	Código PMVV: 6.06.14.0199.3 Serviço de Licenciamento de uso da solução de software Antivírus com atualização continuada, conforme especificações contidas em Termo de Referência - Endpoints (Desktop)	ESET PROTECT ENTERPRISE- 36 meses	Und.	5715	R$249,00	R$1.423.035,00
02	Código PMVV: 6.06.14.0200.0 Serviço de Licenciamento de uso da solução de software Antivírus com atualização continuada, conforme especificações contidas em Termo de Referência – Endpoints (Servidores)	ESET PROTECT ENTERPRISE- 36 meses	Und.	250	R$299,00	R$74.750,00
03	Código PMVV: 6.06.14.0201.9 Licenciamento de uso da solução de AntiSpam com atualização continuada, conforme especificações contidas em Termo de Referência	ESET PROTECT ENTERPRISE- 36 meses	Und.	5715	R$59,00	R$337.185,00

> Em análise ao produto ofertado pela arrematante, identificamos que o produto ESET Protect Enterprise não fornece o serviço de proteção de Anti-Spam.
>
> Realizamos as comparações do ITEM-03 do Edital com base na solução ESET MAIL SECURITY.



	PROTECT ENTRY	PROTECT ADVANCED	PROTECT COMPLETE	PROTECT ENTERPRISE	PROTECT MAIL PLUS
Security Management	✓	✓	✓	✓	✓
Endpoint Protection	✓	✓	✓	✓	✗
File Server Security	✓	✓	✓	✓	✗
Full Disk Encryption	✗	✓	✓	✓	✗
Cloud Sandbox	✗	✓	✓	✓	✓
Mail Security	✗	✗	✓	✗	✓
Cloud App Protection	✗	✗	✓	✗	✗
Endpoint Detection & Response	✗	✗	✗	✓	✗
	EXPLORE SOLUTION	EXPLORE SOLUTION	EXPLORE SOLUTION	EXPLORE SOLUTION	EXPLORE SOLUTION

Documentações utilizadas:

https://www.eset.com/int/business/enterprise-protection-bundle/#system-requirements

https://www.eset.com/fileadmin/ESET/INT/Pages/Business/Bundles/brochure_eset_protect_enterprise_preview.pdf

https://www.eset.com/int/business/solutions/learn-more-about-endpoint-protection/#c6904401

https://help.eset.com/ees/8/pt-BR/?idh_config_epfw_basic_group.html

https://help.eset.com/ees/6/en-US/index.html?idh_config_extension.htm

https://www.eset.com/fileadmin/ESET/INT/Docs/Business/Product-Overview-ESET-Endpoint-Security.pdf

https://help.eset.com/efsw/8.0/pt-BR/getting_started.html

Além do que foi explicitado acima, segue abaixo os itens descritos no edital que não foram identificados na documentação pública do fabricante ESET.

2.2.1 ITEM 01 - SOLUÇÃO DE SEGURANÇA DO TIPO ENDPOINT PROTECTION (ANTIVÍRUS)

2.2.1.1.1. Proteção contra execução de aplicações maliciosas (Application Control) ou similares.

Fontes:

https://forum.eset.com/topic/21905-application-control-or-whitelisting-features-in-the-future/

https://www.eset.com/fileadmin/ESET/INT/Docs/Business/Product-Overview-ESET-Endpoint-Security.pdf

2.2.1.1.8. A funcionalidade de emulação para malware ou similar, deve ter suporte para as plataformas Windows (32 e 64 bits), Linux (32 e 64 bits) e Mac (32 e 64

bits), ou possuir tecnologia para análise de ameaças desconhecidas em ambiente controlado em nuvem própria do fabricante.

Fonte:

https://www.eset.com/int/business/enterprise-protection-bundle/

Não encontramos na documentação pública do Fabricante nenhuma informação referente a compatibilidade com sistemas operacionais Linux de 32 bits.

2.2.1.1.9. A solução deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de 0 Day (dia zero), mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades a seguir: a) SEHOP - Structured Exception Handler Overwrite Protection ou similar; b) Heap Spray (Exploits que iniciam através do HEAP) ou similar; c) Java Exploit Protection; Não encontramos nenhuma documentação que deixe explicita a capacidade da solução de detectar e bloquear os comportamentos do item acima.

2.2.1.1.10. A solução deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code" e suas variantes, assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem para aplicações, sistemas e sistemas operacionais contra exploração de vulnerabilidades conhecidas.

2.2.1.1.19. Permitir configurar quais tipos de arquivos serão verificados (ex: arquivos comprimidos, arquivos auto descompactáveis, .PST, arquivos compactados por compactadores binários, executáveis, cab, msi e outros).

2.2.1.1.20. Capacidade de impedir a execução ou instalação de aplicativos e softwares que constam na black list (lista negra).

Não encontramos na documentação da solução nenhuma informação referente aos itens acima.

2.2.2 ITEM 02 - SOLUÇÃO DE SOFTWARE ANTIVÍRUS - ENDPOINTS (SERVIDORES)

2.2.2.1.2 Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux;

Não encontramos nenhuma documentação que deixe explicita a capacidade da solução de detectar e bloquear o comportamento do item acima.

2.2.2.1.3. Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização para criação de regras avançadas.

2.2.2.1.7. A solução deve fornecer o escaneamento e envio de atualizações de vacinas, regras, políticas, patches virtuais e outras para todos os servidores.

2.2.2.1.9 Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando regras de monitoramento de acordo com o resultado desta varredura;

2.2.2.1.10. Ser compatível para gerenciamento de máquinas virtuais nos ambientes VMware e HyperV;

Não encontramos na documentação da solução nenhuma informação referente ao item acima.

Fonte:

https://www.eset.com/int/business/enterprise-protection-bundle/#system-requirements

2.2.2.1.16 O software de proteção deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem de sistemas e aplicações contra exploração de vulnerabilidades conhecidas; Não encontramos nenhuma documentação que deixe explicita a capacidade da solução de detectar e bloquear o comportamento do item acima.

2.2.2.1.17 Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web da CONTRATANTE, inclusive sistemas legados;

2.2.2.1.23. Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O. e demais aplicações, recomendando ações para blindagem de vulnerabilidades existentes no S.O. e aplicações.

2.2.2.1.27. A solução deverá suportar a tecnologia hiperconvergente Nutanix

2.2.2.2.3. A solução deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros (ferramentas para BI, por exemplo).

2.2.2.2.10. Controle de Aplicações (Application Control) ou similar, com capacidade de criação de regras e políticas personalizadas definindo quais aplicativos ou sistemas podem ou não ser executados pelos usuários.

Não encontramos na documentação da solução nenhuma informação referente ao item acima.

Fontes:

https://forum.eset.com/topic/21905-application-control-or-whitelisting-features-in-the-future/

https://www.eset.com/fileadmin/ESET/INT/Docs/Business/Product-Overview-ESET-Endpoint-Security.pdf

2.2.2.2.40. Permitir configurar o consumo de recursos que será utilizado para varreduras.

Não encontramos na documentação da solução nenhuma informação referente ao item acima.

ITEM 03 - SERVIÇO DE LICENCIAMENTO DE USO DA SOLUÇÃO DE ANTISPAM COM ATUALIZAÇÃO CONTINUADA

2.2.3.3.1. Deverá suportar tráfego de entrada e saída de mensagens de no mínimo 5.000.000 mensagens por dia;

2.2.3.3.2. A solução deve ser dimensionada para atender no mínimo 4.000 caixas postais.

2.2.3.4. Controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor.

2.2.3.5. Inspeção e bloqueio de mensagens baseados em tamanho de mensagem, volume de mensagens por período, número de destinatários por mensagem, número de destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP.

2.2.3.9. Proteção contra-ataques de diretório (Directory Harvest Attack), técnica de busca, descoberta e validação de endereços de e-mail no domínio por força bruta.

2.2.3.10. Implementação de recursos de controle de taxa, limitando a quantidade de e-mail aceitos de um emissor específico durante um período de tempo.

2.2.3.15. Categorização de mensagens de saída a partir de políticas preestabelecidas.

2.2.3.22. Implementação de recurso que permita o usuário administrar a sua própria quarentena, dando a opção de bloqueio, encaminhamento e quarentena.

2.2.3.23. Implementação de recurso de cadastro de lista negra (black list) e lista branca (white list) pelo próprio usuário.

2.2.3.26. Implementação de inserção de carimbo no assunto de mensagens e de texto no corpo de mensagens.

2.2.3.29. A instalação da solução deve ser compatível com, no mínimo, os seguintes sistemas operacionais:

2.2.3.29.2. Linux nas versões (32 e 64 bits).

2.2.3.34. Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas.

2.2.3.35. Deve ter a capacidade de rejeitar conexões que tentem ser abertas pelos comandos "HELO" e "EHLO", sem que existam gravados seus endereços de "MX" e "A" nos servidores de DNS.

2.2.3.39. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego.

Não encontramos na documentação da solução nenhuma informação referente aos itens acima.

2.2.3.40. Atualização automática dos filtros sem interrupção dos serviços e/ou perda das regras pré-estabelecidas pelo administrador.

Na documentação é informado que em alguns casos pode ser necessário realizar a reinicialização do servidor após a atualização dos componentes.

2.2.3.42. A solução deverá possuir um sistema que permita estabelecer uma reputação (pontuação) dos endereços IP de servidores que estarão iniciando conexões TCP. Após estabelecida essa reputação, a solução deverá permitir ações diferenciadas de acordo com a pontuação obtida.

2.2.3.43. O administrador deverá ter a possibilidade de aplicar políticas por meio de pontuação podendo aplicar ações. Não encontramos na documentação da solução nenhuma informação referente ao item acima.

2.2.3.44. O sistema de verificação de reputação não deverá basear-se somente em RBL's públicas. Na documentação não é informado uma maneira de inserir manualmente a reputação dos objetos.

2.2.3.46. A solução deverá possuir proteção contra-ataques dos tipos:

2.2.3.46.1. Negação de Serviço (DDoS);

2.2.3.46.3. Ataques de diretório (Directory Harvest Attack). Não encontramos nenhuma documentação que deixe explicita a capacidade da solução de detectar e bloquear os comportamentos do item acima. A solução após o escaneamento deverá incluir, no mínimo, as seguintes ações:

2.2.3.54.5. Envio de mensagem de notificação para um outro endereço, inclusive o destinatário;

2.2.3.58. A solução deverá suportar vários domínios (registros MX), e suportar roteamento de mensagens baseado em cada um desses domínios.

2.2.3.59. A solução deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena.

2.2.3.60. Especificações Técnicas de Console e Gerenciamento - Solução de Antispam Não encontramos na documentação da solução nenhuma informação referente ao item acima.

2.2.3.60.1. A console deve possuir integração com LDAP's e com o serviço de diretório Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores. Não identificamos na documentação nenhuma indicação de que a solução possui qualquer tipo de integração com servidores LDAP.

2.2.3.60.4. A solução deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros (ferramentas para BI, por exemplo). Não encontramos na documentação da solução nenhuma informação referente ao item acima.

2.2.3.60.5. A solução deve possibilitar a monitoração e geração de relatórios a partir da console de administração nos formatos PDF, HTML, CSV ou TXT, com a possibilidade de envio por email.

Na documentação é mencionada apenas a possibilidade de geração de relatórios nos formatos TXT e CSV.

2.2.3.60.6. A solução deve possibilitar a criação de dashboards personalizados.

2.2.3.60.28. A solução deverá permitir o gerenciamento das filas de mensagens (queues), visualizando-as e com as opções de parar e iniciar as filas e de excluir mensagens.

Não encontramos na documentação da solução nenhuma informação referente ao item acima.

Oportuno registrar que, antes de deliberar pela desclassificação da proponente, realizamos diligências em diversos sites, cujas fontes foram indicadas acima. Desta forma, considerando que a solução proposta não atende aos requisitos mínimos exigidos no instrumento convocatório, opinamos pela DESCLASSIFICAÇÃO da empresa BRINFOR SOLUÇÕES EM TI LTDA.

Diante das razões expostas no parecer emitido pelo setor técnico da Secretaria Municipal de Tecnologia e Informação, fica a empresa BRINFOR SOLUÇÕES EM TI LTDA desclassificada do lote do PE 119/2021.

Em 08 de Outubro de 2021

Ivo Pereira Bastos Neto
Pregoeiro Municipal
Central de Compras Governamentais/SEMPLAPE