

Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 50500.154195/2022-68

2. Descrição da necessidade

O presente documento visa a contratação de empresa especializada para fornecimento de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.

Atualmente a ANTT utiliza solução de antivírus tradicional (Windows Defender) que, diante da sofisticação dos ataques digitais e de novas ameaças que não se restringem apenas a artefatos maliciosos (códigos executáveis e artefatos embutidos em arquivos), não mais está apta a proteger o ambiente da Agência, visto que as assinaturas de ataque estão cada vez mais modernas e órgãos governamentais estão frequentemente sendo alvos de ataques cibernéticos. As tentativas de ataques são direcionadas e coordenadas, muitas vezes com a utilização de ferramentas do próprio sistema operacional, a exemplo de Fileless e Attacks, sendo cada vez mais comuns. Esses ataques têm causado prejuízos a grandes organizações ao redor do mundo, fazendo-se necessária, para Agência, a adição de mais uma camada de tecnologia que prevê a proteção para estes novos tipos de ataques digitais.

A ANTT lida diariamente com uma grande diversidade de informações, das quais muitas são protegidas por lei. A presente contratação tem por objetivo atender demandas relacionadas à proteção de dispositivos, somada a outros esforços, utilizando como referência os padrões ABNT NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação.

O processo de detecção e resposta a estes tipos de ameaças e tentativas de ataques sofisticados, necessita de tecnologias mais avançadas, baseadas em comportamento e inteligência artificial, capazes de detectar anomalias na execução de processos e operações que, muitas vezes, não são percebidas pelas soluções tradicionais.

Diante disso, o cenário, exige um complemento da tecnologia atualmente utilizada pela ANTT, com soluções de nova geração, cujo aparato tecnológico seja mais inteligente e capaz de detectar estes desvios de comportamento no ambiente operacional, com capacidade de mitigação imediata e disponibilidade de instrumentos para investigação da causa raiz do problema, de maneira a proteger o ambiente de novos ataques.

Ademais, foram realizados vários investimentos na concepção e adoção de sistemas internos estruturantes, além da aquisição de vários dispositivos como servidores de rede físicos e virtuais para serviços de e-mail, aplicações estruturantes, armazenamento de arquivos, além de inúmeras estações de trabalho, integrando seu uso em vários processos eletrônicos, melhorando a gestão, a transparência e a agilidade dos serviços prestados pela ANTT, e como consequência, torna-se importante proteger todos os dispositivos utilizados pela Agência, em especial a camada de estações de trabalho e servidores de rede corporativos, que são constantemente utilizados conectados à redes públicas e internas, ficando expostos a todo tipo de ameaças e infecções digitais oriundas da Internet.

Diante do exposto, há a necessidade de contratação de solução de proteção de dispositivos e resposta a ataques cibernéticos, e possibilitar a atualização tecnológica atualmente em uso na Agência, aumentando a segurança e proteção do parque computacional e do ambiente de rede da ANTT.

3. Área requisitante

Área Requisitante	Responsável
Gerência de Infraestrutura Tecnológica	Victor Hugo Gouveia De Lucena Lima

4. Necessidades de Negócio

A contratação pretendida encontra-se alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação da ANTT - PDTIC 2021-2024, ao Planejamento Estratégico Institucional - PEI, de acordo com o Mapa Estratégico da ANTT 2020-2030, e ao Plano Anual de Contratações - PAC 2022, conforme abaixo:

Alinhamento ao Planejamento Estratégico Institucional - PEI			
Planejamento Estratégico ANTT - 2020-2030			
ID	Objetivo Estratégico		
OPG 4	Potencializar a capacidade de inovação e absorção de tecnologias de forma estruturada		
PR2	Aprimorar a disponibilidade, a qualidade e a integração das informações internas e externas		
Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC			
Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2021-2024			
ID	NECESSIDADE		
N7	Propor a modernização das tecnologias utilizadas nos sistemas de informação com uso de mecanismos inovadores		
N10	Aperfeiçoar os mecanismos e ambientes para assegurar alta disponibilidade e evolução tecnológica		
ID	Ação do PDTIC	ID	Meta do PDTIC associada
-	Definir padrões de qualidade com vistas a aprimorar a aquisição ou desenvolvimento das soluções	-	Implementar soluções com uso de inteligência artificial
-	Executar os serviços de gestão e manutenção de infraestrutura: dados em nuvem, site redundante, rede de dados, banco de dados, segurança.	-	Garantir disponibilidade das aplicações: 99%
Alinhamento ao Plano Anual de Contratações - PAC			
Item no PAC	Descrição	Aprovação	
3.42	Solução de proteção de dispositivos e resposta a ataques cibernéticos	Aprovado na Revisão do Planejamento Anual de Contratações - PAC 2022, nos termos da Deliberação nº 171, de 10 de maio de 2022.	

5. Necessidades Tecnológicas

Fornecimento de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento, visando prover ao Agência Nacional de Transporte Terrestre - ANTT a proteção de seus ativos, da eficiência e do controle de qualidade de suas operações, aumentando assim a segurança tecnológica no ambiente computacional da ANTT.

Contratar uma solução que possibilite sua administração de forma centralizada a partir de sua console única de administração em nuvem, possibilitando um gerenciamento único das partes integradas necessárias a seu funcionamento, com características de controle e correção de possíveis vírus digitais baseado em comportamento e inteligência artificial, com capacidade de resposta aos incidentes que ocorrerem, privilegiando fazer com menos estrutura, reduzindo custos com sala-cofre, site-backup,

infraestrutura de hardware, software e recursos humanos internos e terceirizados que estariam envolvidos em sua sustentação e manutenção, além da redução dos custos com depreciação e atualização de versões e pré-requisitos de funcionamento.

Continuidade de Negócio – Aquisição de solução que aumente a segurança e proteção dos dispositivos que compõem o parque computacional e o ambiente de rede da ANTT, fornecendo à equipe de TI alertas para tomada de ações quanto a correção de vulnerabilidades e infecções digitais.

A solução deverá possuir painel gráfico em nuvem em tempo real para acesso via browser possibilitando analisar informações das atividades de proteção e possíveis ataques e/ou vulnerabilidades encontradas nos dispositivos do ambiente computacional da ANTT.

A solução deverá aumentar a prevenção e a remediação em relação a ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais em todos os dispositivos da ANTT protegidos pela solução.

A solução deverá melhorar o controle e a prevenção de ameaças que utilizam amplo espectro de técnicas de coleta de inteligência, não se restringindo a um único arquivo binário malicioso em qualquer dispositivo da ANTT, Windows, Linux.

A solução deverá possibilitar o aumento da mitigação de riscos de ameaças em todo ambiente computacional da ANTT e seus dispositivos, que utilizam falhas recentes e não divulgadas dos sistemas operacionais (0-day exploits).

A solução deverá proporcionar em todos os dispositivos do ambiente da ANTT, a prevenção e remediação de tipos de ameaça que usam técnicas de dividir o ataque em diversas fases podendo, por exemplo, controlar um grande número de equipamentos para diferentes finalidades, de modo que diferentes partes da infraestrutura-alvo sejam utilizadas em cada uma das fases do possível ataque.

A solução deverá reduzir o risco de ameaças que utilizam técnicas de persistência com o direcionamento do ataque conduzido por uma interação e um monitoramento contínuo, até que se alcance um objetivo de invasão e ataque, não buscando apenas oportunidades eventuais nos dispositivos da ANTT.

A solução deverá prover a melhoria e automação dos fluxos de trabalho, onde seja possível deixar de serem realizados manualmente pelas equipes de TI da ANTT, reduzindo os prazos de execução e custos operacionais e aumentar a economia de recursos pela simplificação dos processos, redução no consumo de recursos humanos e melhoria nos fluxos de trabalho, em especial por passar a não ser mais necessário administrar vacinas pois a tecnologia pretendida é baseada em inteligência artificial.

A solução deverá possuir uma console de administração que seja acessível em qualquer ponto da rede da ANTT, inclusive se houver conexão a redes públicas sem a necessidade de uma conexão privada (VPN).

A solução deverá possibilitar sua administração totalmente em nuvem sem a necessidade de instalar ferramental local para seu gerenciamento, sendo local apenas os sensores/agentes.

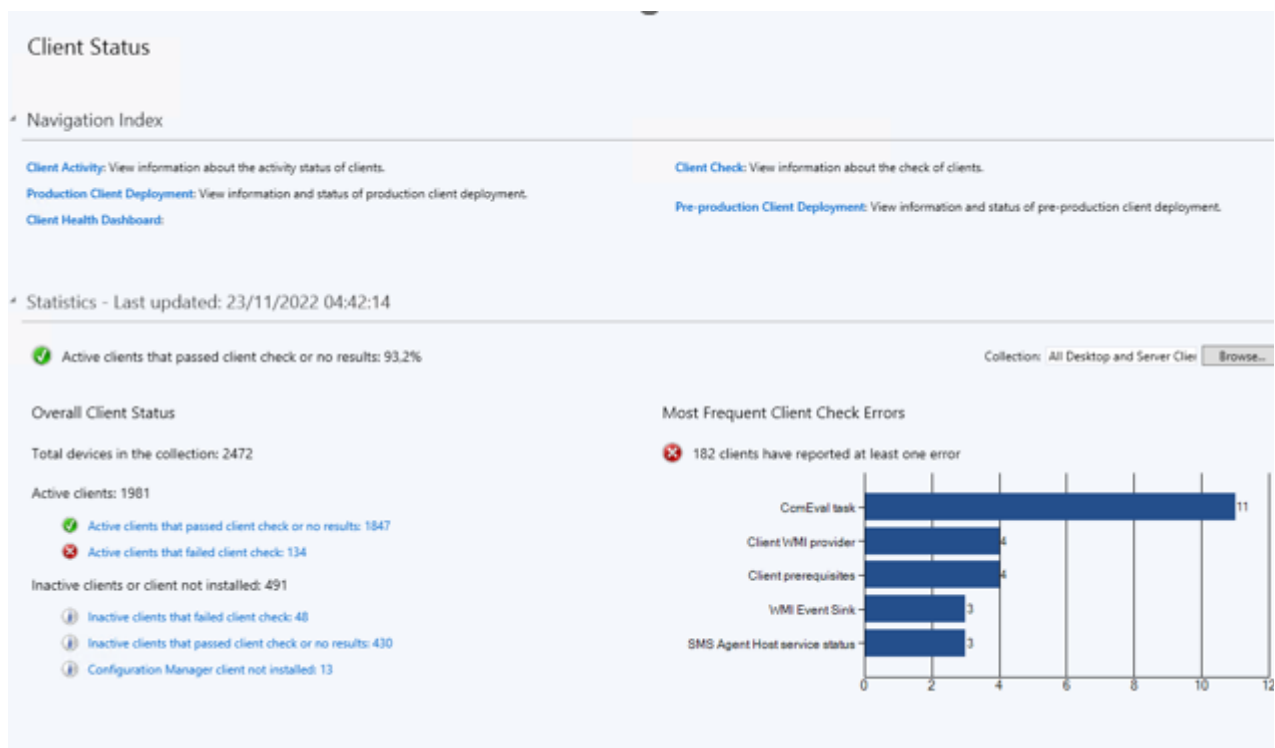
A solução deverá ser em nuvem e deverá necessariamente cumprir pelo menos os requisitos exigidos no item 5 da certificação PCI-DSS V3.2 (Padrão de segurança de dados do setor de cartões de pagamento para organizações de qualquer local do mundo que lidam com cartões de crédito de marca das principais bandeiras/marcas de cartões).

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

O detalhamento técnico da solução encontra-se descrito no **APÊNDICE “A”**, deste Estudo Técnico (SEI nº 13588484).

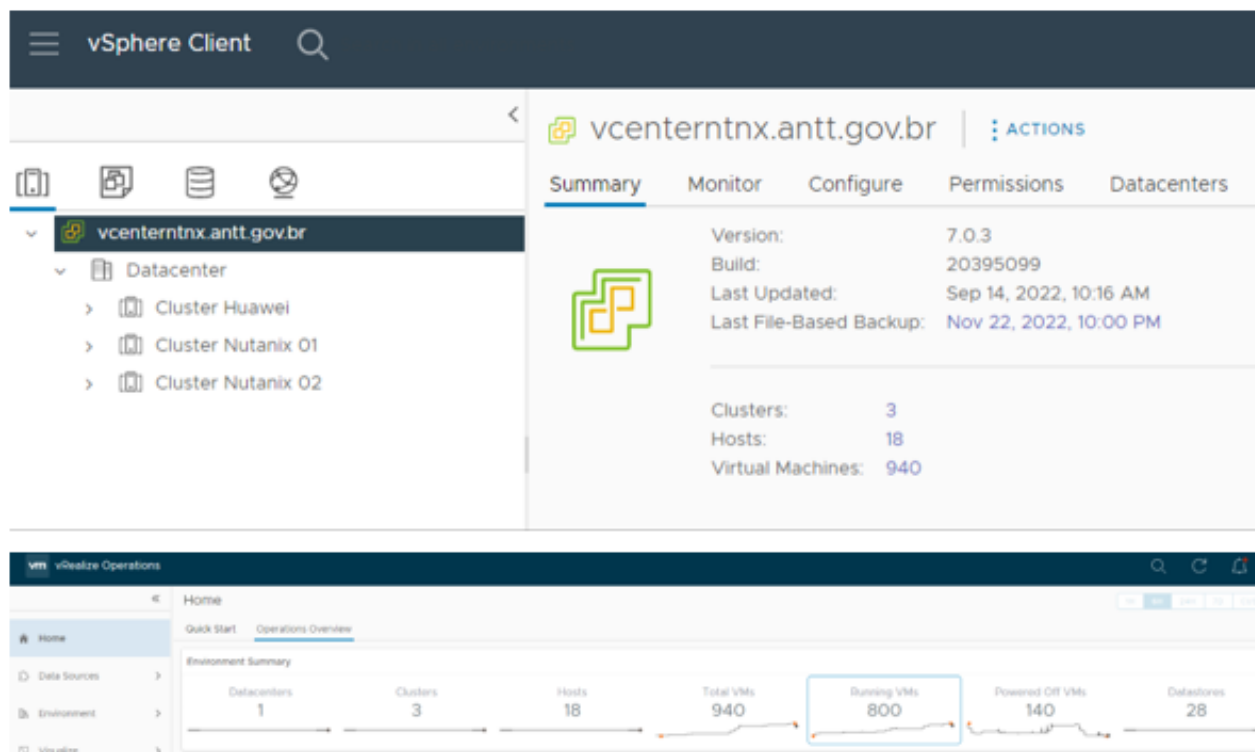
7. Estimativa da demanda - quantidade de bens e serviços

Para o correto dimensionamento da quantidade de subscrições a serem contratadas, a equipe de planejamento da contratação considerou os relatórios abaixo:



Os dados foram extraídos do Microsoft System Center Configuration Manager – SCCM, plataforma que reúne informações a respeito do ambiente computacional da ANTT.

Pelo relatório pode-se observar um total de 2.472 devices, que correspondem às estações de trabalho (endpoints) atualmente ativas no ambiente de rede da Agência. Já os relatórios abaixo foram extraídos da plataforma de virtualização - VSPHERE - utilizada para realizar a gestão dos servidores provisionados pela Agência.



O relatório evidencia um total de 940 servidores virtuais e 18 hosts físicos (um total de 958 servidores), sendo que desses, 800 estão em operação.

O quantitativo estimado a ser contratado refere-se ao somatório do número de estações de trabalho (endpoints) com o número total de servidores em operação. Assim sendo, a estimativa da demanda deverá observar o quantitativo da tabela abaixo:

Item	Descrição	Unidade	Quantidade
1	Serviço anual de Subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimento.	Dispositivo	3.300

8. Levantamento de soluções

Foram identificadas as seguintes soluções para atender as necessidades:

Solução	Descrição
---------	-----------

Solução A - Desenvolvimento próprio da solução através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades.	Cenário que visa o desenvolvimento próprio da solução pela ANTT.
Solução B - Solução de Software Livre	Cenário que visa a contratação de soluções de software livre.
Solução C - Solução (software proprietário) com licenciamento pago por subscrição/aluguel.	Cenário que visa a contratação de solução com licenciamento pago por subscrição/aluguel.

9. Análise comparativa de soluções

Com base nas possíveis soluções identificadas, segue a análise abaixo:

Solução A - Desenvolvimento próprio da solução através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades

Trata-se do desenvolvimento internamente na Agência através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades.

Solução A	
Descrição	Desenvolvimento próprio da solução através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades.
	<p>Essa alternativa é caracterizada pelo desenvolvimento próprio dessa solução na Agência, por meio de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades. No entanto, analisando-se a relação custo-benefício, percebe-se que uma solução com essas características seria altamente custosa/onerosa para ser desenvolvida internamente por meio do contrato de Fábrica de Software vigente.</p> <p>Além disso, em se tratando da possibilidade de desenvolvimento da solução com a utilização da fábrica de software contratada pela Agência, a não utilização dessa solução é justificada ainda pelo fato de que o Ministério da Economia, traz orientações pela publicação do manual "<i>Boas práticas, vedações e orientações para contratação de serviços de desenvolvimento e manutenção de software (Fábrica de Software)</i>", disponível em desenvolvimento e manutenção de software, o seguinte:</p>

<p>Análise da Solução</p>	<p>1. Antes de decidir pela contratação de serviço de desenvolvimento de software ou pela abertura de projetos de desenvolvimento de software, a Equipe de Planejamento da Contratação ou a Equipe de Gestão de Projetos do órgão deve realizar Estudo Técnico Preliminar, nos termos do disposto no art. 12 da Instrução Normativa SLTI/MP nº 4, de 11 de setembro de 2014, e executar as seguintes atividades:</p> <p>1.5. Analisar a viabilidade de contratação de software proprietário.</p> <p>3.5. É vedada a utilização dos serviços contratados para o desenvolvimento de softwares de atividades-meio.</p> <p>3.5.1. São considerados softwares de atividades-meio os que são utilizados para apoio de atividades de gestão ou administração operacional, como, por exemplo, softwares de recursos humanos, ponto eletrônico, portaria, biblioteca, gestão de patrimônio, controle de frotas, gestão eletrônica de documentos, e que não têm por objetivo o atendimento às áreas finalísticas para a consecução de políticas públicas ou programas temáticos.</p> <p>3.5.2. Os softwares de atividades-meio devem ser adquiridos no mercado por meio de adoção de software público ou livre, contratação de software como serviço, ou software licenciado</p> <p>O desenvolvimento de uma solução para atender ao objetivo deste estudo está alinhada à vedação exposta no item 3.5 do manual. Diante do exposto, não é recomendado o desenvolvimento interno da solução. Além disso, importante destacar que o custo-benefício para desenvolvimento interno de uma solução deste tipo com todas as funcionalidades necessárias não seria viável técnica e economicamente.</p> <p>Pelos motivos apresentados, este cenário não é recomendado para atender as necessidades da ANTT.</p>
----------------------------------	---

Solução B - Solução de Software Livre

Software livre é um tipo de software que vem com permissão para cópia, uso e distribuição, com ou sem modificações, de forma gratuita ou por um preço. De forma geral, isso significa que o código-fonte deve estar disponível. A maioria dos softwares livres é licenciada por meio de uma licença livre, sendo o tipo GNU GPL a mais conhecida.

As licenças de software livre permitem que eles sejam vendidos, mas estes em sua grande maioria estão disponíveis gratuitamente.

Abaixo são apresentadas algumas soluções de software livre, porém todas pouco aderentes ao que se deseja dessa contratação:

	<p>Programa gratuito para Windows não sendo necessário grandes configurações.</p>
--	---

<p>Ad-Aware</p> <p>https://www.adaware.com/free-antivirus-download</p>	<ul style="list-style-type: none"> • Pode usado de graça apenas para uso individual. • Só funciona em Windows 10. • Não atende a grande maioria das exigências técnicas mínimas que a ANTT espera de uma solução de proteção de dispositivos. <p>* Não atende a grande maioria dos requisitos mínimos esperados.</p>
<p>Avira</p> <p>www.avira.com/pt-br</p>	<p>Programa gratuito para windows.</p> <ul style="list-style-type: none"> • Limitado gratuitamente a 1 dispositivos. • Não usa machine learning ou inteligência artificial. <p>* Não atende a grande maioria das necessidades.</p>

Existem outros softwares livres que poderiam atender parte dos requisitos levantados pelo requisitante da solução, mas não há uma ferramenta que atenda toda a necessidade ou grande parte dos requisitos, além de não proverem a solução em nuvem.

Solução B	
Descrição	Solução de Software Livre
Análise da Solução	<p>Foram encontradas algumas soluções de software livre, porém todas pouco aderentes ao que se deseja dessa contratação:</p> <p>Ad-Aware - https://www.adaware.com/free-antivirus-download</p> <p>Programa gratuito para Windows não sendo necessário grandes configurações.</p> <ul style="list-style-type: none"> • Pode usado de graça apenas para uso individual. • Só funciona em Windows 10. • Não atende a grande maioria das exigências técnicas mínimas que a ANTT espera de uma solução de proteção de dispositivos. <p>* Não atende a grande maioria dos requisitos mínimos desejados.</p> <p>Avira - www.avira.com/pt-br</p> <p>Programa gratuito para windows.</p> <ul style="list-style-type: none"> • Limitado gratuitamente a 1 dispositivos. • Não usa machine learning ou inteligência artificial.

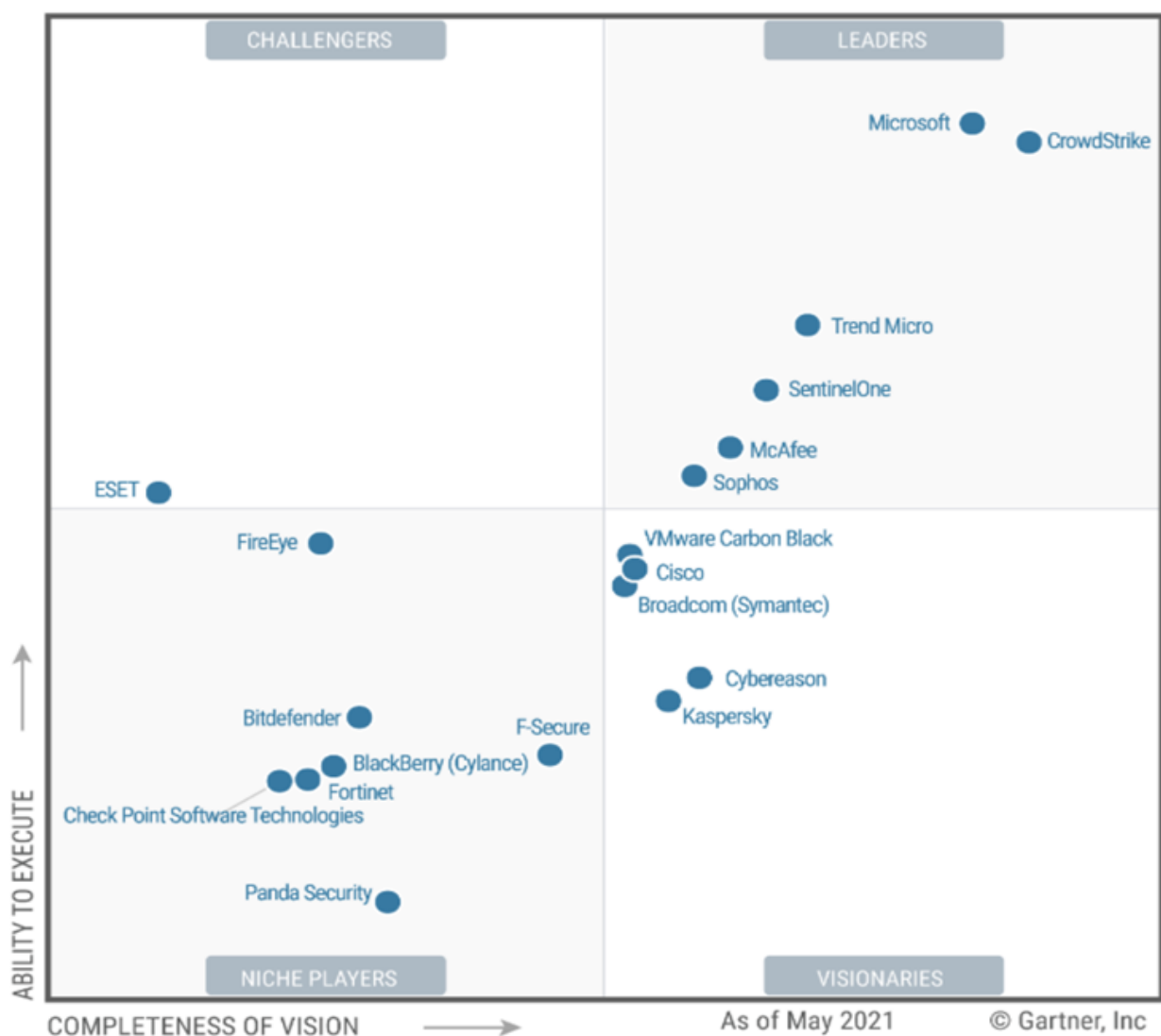
* Não atende a grande maioria das necessidades.

Pelos motivos apresentados, a equipe entende que a Solução de Software Livre, não se mostra adequada para o cenário atual das necessidades tecnológicas da ANTT.

Solução C - Solução (software proprietário) com licenciamento pago por subscrição/aluguel.

A seguir apresentamos algumas soluções identificadas através de buscas na Internet ou pela leitura de estudos de mercado utilizados pelo Gartner.

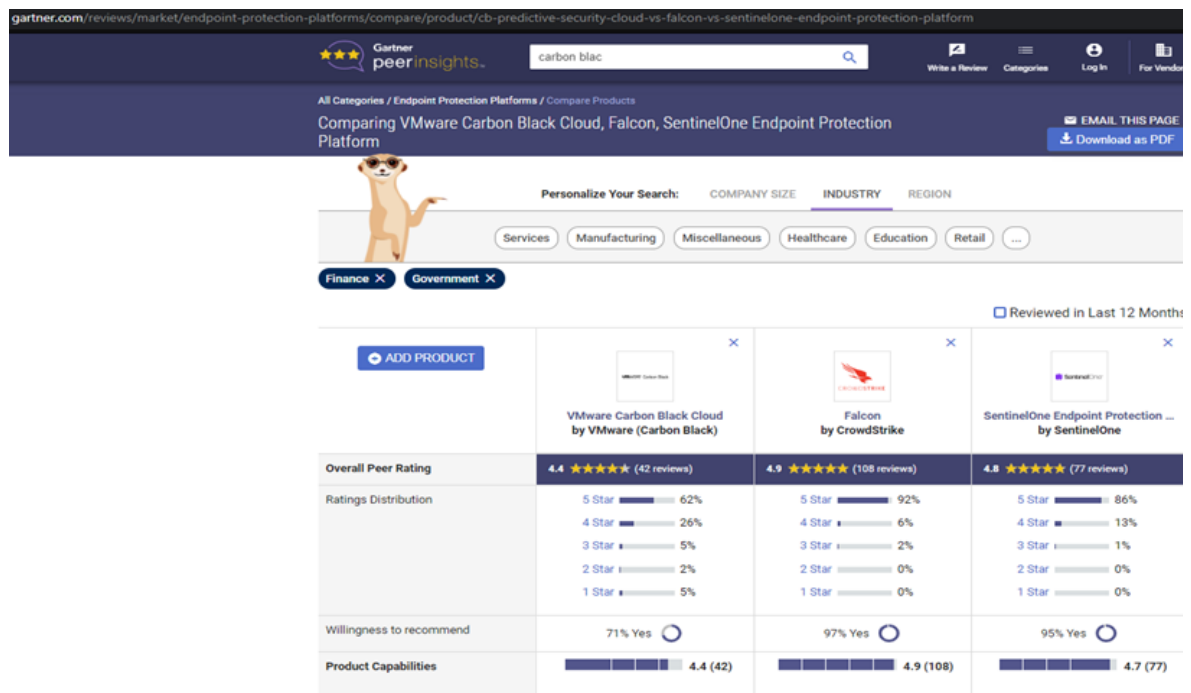
Figure 1: Magic Quadrant for Endpoint Protection Platforms



Além disso, a equipe técnica apresenta exemplos de fabricantes que possivelmente podem atender as demandas da contratação, são eles:

- Carbon black - <https://www.carbonblack.com/>
- SentinelOne - <https://www.sentinelone.com/>

- CrowdStrike - <https://www.crowdstrike.com/>



Após consultas ao mercado de tecnologia por meio de solicitações de cotações, ficou evidente que a modalidade por subscrição anual de soluções em nuvem melhor atende a Agência, pois além de manter toda solução atualizada em suas últimas versões disponíveis, de forma automática, atende as necessidades levantadas.

Pelos motivos apresentados, este cenário é o recomendado para atender as necessidades da ANTT.

Dessa forma, e de acordo com as necessidades levantadas após realização de estudos, a equipe técnica conclui que somente a Solução C (software proprietário) com licenciamento pago por subscrição/aluguel, poderá atender as necessidades da Agência.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução A		X	
	Solução B			X
	Solução C		X	
	Solução A		X	

A Solução está disponível no Portal do Software Público Brasileiro?	Solução B		X	
	Solução C		X	
A Solução é composta por software livre ou software público?	Solução A		X	
	Solução B	X		
	Solução C		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução A	X		
	Solução B	X		
	Solução C	X		
A Solução é aderente às regulamentações da ICP-Brasil?	Solução A			X
	Solução B			X
	Solução C			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução A			X
	Solução 2			X
	Solução 3			X

Contratações similares realizadas por outros órgãos ou entidades da Administração Pública

Com base nos parâmetros dispostos na IN nº 73/2020, foram realizadas consultas no Painel de Preços/Comprasnet (SEI nº 13589483 e 13589526) e com a Administração Pública (SEI nº 13589551), sendo identificado os seguintes resultados aderentes ao objeto:

Análise consulta painel de preços/comprasnet/Administração Pública

PREGÃO	ORGÃO	UASG	ANÁLISE
5/2021	Banco da Amazônia S/A - BA	179007	Objeto similar ao pretendido pela Agência. Referência utilizada.
46/2021	Procuradoria Geral de Justiça do Piauí - PGJ/PI	926092	Objeto similar ao pretendido pela Agência. Referência utilizada.
4/2021	Instituto de Pesquisa Econômica Aplicada - IPEA	113601	Objeto similar ao pretendido pela Agência. Porém, com garantia e suporte técnico pelo período de 36 meses. Referência não utilizada.
7/2021	Tribunal de Contas Mato Grosso - TC/MT	972002	Objeto similar ao pretendido pela Agência. Porém, com garantia e suporte técnico pelo período de 24 meses. Referência não utilizada.
28/2021	Universidade Federal da Bahia - UF/BA	153038	Objeto similar ao pretendido pela Agência. Porém, com garantia e suporte técnico pelo período de 36 meses. Referência não utilizada.
4/2022	Conselho Regional de Contabilidade do Rio de Janeiro - CRC/RJ	383518	Objeto similar ao pretendido pela Agência. Porém, com garantia e suporte técnico pelo período de 36 meses. Referência não utilizada.
65/2022	Secretaria Municipal de Educação - PM/SP	925013	Objeto diferente (capas de proteção e películas de proteção para dispositivos) do pretendido pela Agência. Referência não utilizada.

Com base nos resultados reportados no painel de preços, órgãos da Administração Pública e Pesquisa a fornecedores, considerando as especificidades do objeto obteve-se os seguintes resultados:

Consolidado consulta painel de preços/comprasnet/Administração Pública + fornecedores

Item	Descrição	Métricas	Quantidade	REFERÊNCIAS							
				A PE nº 05/2021 BA		B PE nº 46/2021 PGJ/PI		C PROPOSTA 1		D PROPOSTA 2	
				Vir. Unit.	Vir. Total (12 meses)	Vir. Unit.	Vir. Total (12 meses)	Vir. Unit.	Vir. Total (12 meses)	Vir. Unit.	Vir. Total (12 meses)
1	Serviço anual de subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimentos.	Dispositivos	3.3.00	125,50	414.150,00	292,25	96.6425,00	599,00	1.976.700,00	615,00	2.029.500,00

Item	Descrição	Métricas	Quantidade	REFERÊNCIAS							
				E PROPOSTA 3		F PROPOSTA 4		G PROPOSTA 5		Média Valor de Referência	
				Vir. Unit.	Vir. Total (12 meses)	Vir. Unit.	Vir. Total (12 meses)	Vir. Unit.	Vir. Total (12 meses)		
1	Serviço anual de subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimentos.	Dispositivos	3.3.00	617,00	2.036.100,00	610,00	2.013.000,00	680,00	2.268.000,00	505,54	1.668.282,00
Valor Total R\$											R\$ 1.668.282,00

Fonte	CNPJ/UASG
A) PE nº 5/2021 - Banco da Amazônia S/A - BA	Uasg: 179007
B) PE nº 46/2021 - Procuradoria Geral de Justiça do Piauí - PGJ/PI	Uasg: 926092
C) PROPOSTA 1 - Centro de Pesquisas em Informática Ltda.	40.584.096/0005-05
D) PROPOSTA 2 - Nova Serviços de Tecnologia da Informação e Networking DIREI	30.645.992/0008-79
E) PROPOSTA 3 - Garagem Brasil LTDA	11.038.368/0005-65
F) PROPOSTA 4 - Global Red Tecnologia da Informação LTDA	07.430.353-0008/29
G) PROPOSTA 5 - Altech Soluções em Tecnologia Ltda	21.547.081/0005-66

Algumas contratações identificadas na pesquisa não foram consideradas na tabela acima, tendo em vista não possuírem similaridade com o objeto.

10. Registro de soluções consideradas inviáveis

Após levantamento das possíveis soluções, a equipe de planejamento da contratação, conclui que as soluções inviáveis correspondem a:

Solução	Descrição
Solução A - Desenvolvimento próprio da solução através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais.	Cenário que visa o desenvolvimento próprio da solução pela ANTT.
Solução B - Solução de Software Livre	Cenário que visa a contratação de soluções de software livre.

Dessa forma, com base no § 1º do art. 11 da IN 01/2019 da SGD/ME, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos, realizada nos termos do inciso III do art. 11 da Instrução Normativa SGD/ME nº 1/2019, baseou-se nas contratações realizadas no âmbito da Administração Pública com objeto similar, bem como em pesquisa direta com o fornecedor da solução.

Cálculo dos custos totais de propriedade para um período de 5 (cinco) anos

ITEM	DESCRIÇÃO	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	CUSTO TOTAL (5 ANOS)
		Valor Total	Valor Total	Valor Total	Valor Total	Valor Total	Valor Total
1	Serviço anual de Subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimento.	1.668.282,00	1.767.711,61	1.873.067,22	1.984.702,03	2.102.990,27	9.396.753,12
(TCO) TOTAL							9.396.753,12

O custo total considerou o ICTI índice jul/2022, no percentual de 5,96% - Fonte: <https://www.ipea.gov.br/cartadeconjuntura/index.php/2022/09/indice-de-custo-da-tecnologia-da-informacao-icti-julho-de-2022/>.

12. Descrição da solução de TIC a ser contratada

O detalhamento técnico da solução de TIC a ser contratada encontra-se no APÊNDICE “A”, deste Estudo Técnico (SEI nº 13588450).

13. Estimativa de custo total da contratação

Valor (R\$): 1.668.282,00

O custo total da contratação resta estimado em R\$ 1.668.282,00 (um milhão, seiscentos e sessenta e oito, duzentos e oitenta e dois mil reais).

14. Justificativa técnica da escolha da solução

Com base nas informações levantadas ao longo do estudo técnico, a equipe de planejamento da contratação concluiu que a contratação da Solução C - (software proprietário) com licenciamento pago por subscrição/aluguel, é a opção que se apresenta mais vantajosa, do ponto de vista técnico e econômico, sendo relevante e essencial para a manutenção e desenvolvimento das atividades, pois, disporá de um painel gráfico em nuvem e em tempo real para acesso via browser, possibilitando analisar informações das atividades de proteção e possíveis ataques, explorando as vulnerabilidades existentes nos dispositivos do ambiente computacional da ANTT.

15. Justificativa econômica da escolha da solução

A solução de proteção de dispositivos é uma necessidade urgente da Agência, e a sua adoção possibilitará a administração de forma centralizada a partir de sua console de administração 100% em nuvem, possibilitando um gerenciamento único das partes integrantes necessárias a seu funcionamento, com características de controle e correção de possíveis vírus digitais baseado em comportamento e inteligência artificial, com capacidade de resposta aos incidentes que ocorrerem.

A solução reduzirá custos com sala-cofre, site-backup, infraestrutura de hardware, software e recursos humanos internos que estariam envolvidos em sua sustentação e manutenção, além da redução dos custos com depreciação e atualização de versões e pré-requisitos de funcionamento.

Dessa forma, a equipe concluiu que a Solução C se mostra mais econômica para atender as necessidades da ANTT.

16. Justificativa do parcelamento da Solução

A solução é composta de um único item.

17. Benefícios a serem alcançados com a contratação

Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

- a) Aumentar a segurança e proteção dos dispositivos que compõem o parque computacional e o ambiente de rede da ANTT, fornecendo à equipe de TI alertas para tomada de ações quanto a correção de infecções digitais que estejam sendo exploradas por atores maliciosos;
- b) Dispor de painel gráfico em nuvem em tempo real para acesso via browser possibilitando analisar informações das atividades de proteção e possíveis ataques explorando vulnerabilidades existentes nos dispositivos do ambiente computacional da ANTT;
- c) Melhorar o controle e a prevenção de ameaças que utilizam amplo espectro de técnicas de coleta de inteligência, não se restringindo a um único arquivo binário malicioso em qualquer dispositivo da ANTT;
- d) Aumentar a prevenção e a remediação em relação a ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia, e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais em todos os dispositivos da ANTT protegidos pela solução;
- e) Possibilitar o aumento da mitigação de riscos de ameaças em todo ambiente computacional da ANTT e seus dispositivos, que utilizam falhas recentes e não divulgadas dos sistemas operacionais (0-day exploits);
- f) Proporcionar em todos os dispositivos do ambiente da ANTT, a prevenção e remediação de tipos de ameaça que usam técnicas de dividir o ataque em diversas fases podendo, por exemplo, controlar um grande número de equipamentos para diferentes finalidades, de modo que diferentes partes da infraestrutura-alvo sejam utilizadas em cada uma das fases do possível ataque;
- g) Reduzir o risco de ameaças que utilizam técnicas de persistência com o direcionamento do ataque conduzido por uma interação e um monitoramento contínuo, até que se alcance um objetivo de invasão e ataque, não buscando apenas oportunidades eventuais nos dispositivos da ANTT;
- h) Evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers, reduzindo o risco dos dispositivos, serviços e sistemas tecnológicos da ANTT serem acessados sem autorização;
- i) Proporcionar consultas para auditoria por meio de Dashboard das detecções mais recentes, a quantidade de novas detecções e as que aconteceram por táticas nos últimos 30 dias, sendo possível reportar de forma agrupada para os dispositivos do ambiente de rede da ANTT.

- j) Prover relatórios de todas as conexões remotas realizadas desde a console de gerenciamento até o dispositivo final gerenciado, contendo informações detalhadas de sua utilização, garantindo o não-repúdio e/ou exclusão de informações;
- k) Prover a melhoria e automação dos fluxos de trabalho, onde estejam sendo realizados manualmente pelas equipes de TI da ANTT, reduzindo os prazos de execução e custos operacionais;
- l) Ampliação da visibilidade, transparência e colaboração corporativa que trazem excelência operacional, alinhamento entre as áreas de TI e Negócio da ANTT e a qualidade de atendimento a seus clientes internos e externos.

18. Providências a serem Adotadas

Elaboração do Plano de Implantação da solução compreendendo a instalação e configuração do software de proteção de dispositivos.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Com base nas informações levantadas ao longo do estudo técnico preliminar, os integrantes requisitante e técnico, da equipe de planejamento, declaram que a contratação da Solução C - (software proprietário) com licenciamento pago por subscrição/aluguel, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento, é viável do ponto de vista técnico e econômico, pois, irá aumentar a segurança e proteção dos dispositivos que compõem o parque computacional e ambiente de rede da Agência.

O presente Estudo Técnico preliminar da Contratação foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019, da Secretaria de Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição.

20. Responsáveis

O presente Estudo Técnico preliminar da Contratação foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019, da SGD.

JOÃO PROCÓPIO DO REGO NETO

Integrante Requisitante

O presente Estudo Técnico preliminar da Contratação foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1 /2019, da SGD.

VICTOR HUGO GOUVEIA DE LUCENA LIMA

Integrante Técnico

APROVO este Estudo Técnico Preliminar e DECLARO sua adequação às disposições da Instrução Normativa SGD/ME nº 1 /2019, da Secretaria de Governo Digital do Ministério da Economia.

DIOGO DA FONSECA TABALIPA

Superintendente de Tecnologia da Informação

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Apêndice A - Requisitos Técnicos Mínimos da Solução.pdf (296.94 KB)

Anexo I - Apêndice A - Requisitos Técnicos Mínimos da Solução.pdf

APÊNDICE "A"**REQUISITOS MÍNIMOS DA SOLUÇÃO****1. DESCRIÇÃO DOS REQUISITOS MÍNIMOS DA SOLUÇÃO**

1.1. Contratação de serviço anual de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento conforme tabela abaixo:

Lote	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
Único	Serviço anual de Subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimento.	Dispositivos	3.300		

2. DESCRIÇÃO DOS REQUISITOS TÉCNICOS OBRIGATÓRIOS

2.1. A console de administração deve ser centralizada para gerenciar todos os dispositivos, independentemente da localização geográfica.

2.2. A console de administração deve ser acessível em qualquer ponto da rede da contratante até mesmo quando estiverem conectados a redes públicas sem a necessidade de uma conexão VPN;

2.3. A solução deverá ser baseada em plataforma de nuvem e oferecida como serviço seguindo boas práticas.

2.4. A administração deve estar acessível através de HTTPS usando pelo menos um dos navegadores abaixo:

- a) Google Chrome;
- b) Edge;
- c) Firefox;

2.5. A administração da solução deverá ser 100% em nuvem sem a necessidade de instalação de ferramenta local para o gerenciamento da solução;

2.6. A gerência de administração da solução deve ter capacidade de separar os dispositivos gerenciados através de grupo via seleção manual e a criação de grupos com adição de dispositivos de forma automática com base em no mínimo, os critérios abaixo:

- a) Domínio;
- b) Endereços IP;
- c) Hostname parcial ou completo;
- d) Versão de sistema operacional;
- e) Unidade Organizacional do Active Directory;
- f) Versão do agente.

2.7. A gerência deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;

2.8. O uso de um fator de autenticação duplo deve ser utilizado para autenticação na console de gerenciamento da solução;

2.9. Deve ser possível a definição de papéis (RBAC) para os usuários dentro da console de administração delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;

2.10. A console de gerenciamento deve oferecer suporte Single Sign On com compatibilidade de pelo menos 3 opções distintas de provedor de identidade (IdP) na qual uma das opções deve ser obrigatoriamente Active Directory Federation Services (AD FS);

2.11. A console deve contemplar, no mínimo, as seguintes visualizações;

- a) Agentes ativos;
- b) Agentes por sistema operacional;
- c) Detecções por objetivo do ataque;
- d) Detecções por tática do ataque;
- e) Detecções por severidade do ataque.

2.12. A solução deverá suportar a instalação de agentes e/ou sensores diretamente no sistema operacional de cada máquina virtual ou diretamente no virtualizador

(hypervisor) sendo as duas formas aceitas;

2.13. A console de administração deve centralizar a administração dos sistemas operacionais Windows, Mac OS e Linux, não sendo aceitas múltiplas consoles para administração;

2.14. A console de gerência central deve ser capaz de atualizar os agentes de forma automática definida via política considerando no mínimo as seguintes opções;

- a) Versão mais recente;
- b) Versão específica;
- c) Uma versão anterior a mais recente (N-1);
- d) Duas versões anteriores a mais recente (N-2);

2.15. A plataforma deverá prevenir e remediar ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais.

2.16. A plataforma em nuvem deverá cumprir com as exigências da acreditação NSA-CIRA (certificando que foi avaliada e certificada em áreas de foco críticas derivadas das práticas recomendadas da indústria e do governo para investigação de segurança cibernética).

2.17. A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes).

2.18. A solução deve possuir um único software agente instalado em cada dispositivo para prover todas as funcionalidades descritas neste documento e que serão administradas através da conexão com a console de gerenciamento. Não será aceita a instalação de componentes adicionais como agentes de comunicação com múltiplos subagentes, plug-ins e softwares de terceiros para o atendimento dos requisitos;

2.19. O agente deve suportar os seguintes sistemas operacionais:

- a) Windows Server 2022;
- b) Windows Server 2019;
- c) Windows Server 2016;
- d) Windows Server 2012 R2;
- e) Windows Server 2012;
- f) Windows Server 2008 R2 SP1;
- g) Windows 11;
- h) Windows 10;
- i) Windows 8.1;
- j) Windows 7 SP1;
- k) Debian 9;
- l) Debian 10;
- m) SUSE Linux Enterprise (SLES) 11.4
- n) SUSE Linux Enterprise (SLES) 12.2 – 12.5
- o) SUSE Linux Enterprise (SLES) 15 – 15.3
- p) CentOS ou Red Hat Enterprise Linux (RHEL) 6.7 - 6.10
- q) CentOS ou Red Hat Enterprise Linux (RHEL) 7.4 - 7.7;
- r) CentOS ou Red Hat Enterprise Linux (RHEL) 8.0 - 8.5;
- s) Red Hat Enterprise Linux (RHEL) 8.6;
- t) Red Hat Enterprise Linux (RHEL) 9.0;
- u) Ubuntu 18.04 LTS;
- v) Ubuntu 20.04 LTS;
- w) Ubuntu 22.04 LTS.

2.20. A comunicação entre o agente e a console de gerenciamento deve utilizar um túnel de segurança TLS criptografado utilizando certificate pinning;

- a) A capacidade de *certificate pinning* implementada no agente não deverá permitir a relação de confiança com o armazenamento de chaves local do sistema operacional, ou seja, mesmo se um certificado raiz for adicionado na keystore local o agente não deverá herdar essa relação de confiança.

2.21. O agente deve suportar comunicação com a console de gerenciamento através de proxy.

2.22. Características específicas para sistemas operacionais Windows

- a) As seguintes opções de proxy deverão ser suportadas pelo agente, suportando no mínimo a combinação de duas ou mais opções ao mesmo tempo;
- b) Proxy configurado manualmente na estação ou via GPO;
- c) PAC configurado manualmente na estação ou via GPO;
- d) WPAD configurado para detectar automaticamente um arquivo PAC via DHCP ou DNS;
- e) Proxy definido no agente.

2.22.1. Quando o agente for configurado para utilizar 2 ou mais das configurações de proxy as mesmas devem ser acumulativas, ou seja, se for configurado proxy específico a nível de agente e o mesmo não estiver disponível ele deverá usar o proxy da estação e em último caso tentar a conexão direta;

2.22.2. Deverá ser possível configurar o agente para utilizar conexão direta, ou seja, ignorar qualquer configuração de proxy existente na máquina;

2.22.3. O agente deve implementar proteção de desinstalação através de token específica para cada dispositivo gerenciado.

2.22.4. Deve detectar tentativas de manipulação indevida dos componentes do agente;

2.22.5. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

2.22.6. Não serão aceitas soluções que utilizem somente assinaturas para reconhecer ameaças;

2.22.7. O ML (Machine Learning) deve realizar a detecção e prevenção de artefatos maliciosos conhecidos e desconhecidos não somente na tentativa de execução, como também na tentativa de escrita do binário em disco, ou seja, se um binário considerado malicioso pelo motor de ML for escrito em disco deverá resultar em uma detecção e prevenção no momento da operação de escrita em disco.

2.22.8. Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.

2.22.9. Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

2.22.10. Deve ser capaz de detectar Adware e programas potencialmente indesejados;

- 2.22.11. Deve ser capaz de detectar ameaças mesmo que o dispositivo não esteja conectado à Internet;
- 2.22.12. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
- 2.22.13. Deve permitir bloqueio de scripts e comandos em Powershell considerados suspeitos;
- 2.22.14. Deve permitir bloqueio automático de processos suspeitos;
- 2.22.15. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;
- 2.22.16. Deve permitir bloqueio de operações em registros suspeitos;
- 2.22.17. Deve permitir que arquivos maliciosos possam ser movidos para uma área de quarentena;
- 2.22.18. Deve possuir integração com o Windows Security Center para ser reconhecido como uma solução de proteção válida para antimalware;
- 2.22.19. Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória;
- 2.22.20. Deve ser capaz de forçar Data Execution Prevention de forma a impedir ataques que utilizem espaço de memória para execução de códigos em região de memória não executável;
- 2.22.21. Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;
- 2.22.22. Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);
- 2.22.23. Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos;
- 2.22.24. Deve ser capaz de detectar malwares do tipo Ransomware com base em, no mínimo, os comportamentos abaixo:
 - a) Deletar backups;
 - b) Operações em excesso ao sistema de arquivos;
 - c) Criptografia de arquivos;
 - d) Processos associados a malwares de ransomware Cryptowall, Wannacry, Locky;
 - e) Processo suspeito de deleção de um volume de “Shadow Copies”

2.22.25. Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos:

2.22.26. Criação de processos suspeitos originados de navegadores;

2.22.27. Detecção de comprometimento de servidores Web através de webshell;

2.22.28. Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;

2.22.29. Injeção de código não esperada de um processo a outro;

2.22.30. Execução de JavaScript através do executável Rundll32.

2.22.31. Deve ser capaz de detectar movimentação lateral através de circunvenção do processo de logon do Windows;

2.22.32. Deve ser capaz de detectar de processos que tentam obter credenciais de login;

2.22.33. A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK;

a) T1003, T1012, T1018, T1021, T1026, T1027, T1036, T1047, T1048, T1049, T1053, T1055, T1059, T1061, T1070, T1087, T1095, T1102, T1110, T1112, T1132, T1133, T1136, T1204, T1218, T1219, T1222, T1482, T1486, T1489, T1490, T1505, T1529, T1543, T1547, T1548, T1550, T1056, T1558, T1559, T1560, T1562, T1564, T1567, T1570, T1571, T1574.

2.22.34. O agente para estações Windows deve suportar a RFC 5246;

2.22.35. Deve permitir que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no dispositivo gerenciado;

2.22.36. Deve permitir exclusão de arquivos e pastas utilizando caracteres coringa (Wildcard);

2.22.37. Deve permitir rodar comandos no dispositivo em tempo real por meio da console de gerenciamento em nuvem, precisando contemplar as seguintes ações:

a) Mostrar as conexões de rede

b) Mostrar os processos ativos

c) Encerrar um processo ativo

d) Reiniciar o dispositivo

- e) Desligar o dispositivo
- f) Acessar e deletar arquivos
- g) Iniciar execução de um processo;
- h) Dump de memória do dispositivo;

2.22.38. Deve permitir a definição granular da execução ou não de, no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no dispositivo via console de gerenciamento;

- a) Extração de arquivos;
- b) Iniciar execução de um processo;
- c) Dump de memória do dispositivo;

2.22.39. Deve permitir que scripts Powershell possam ser adicionados à solução para que possam ser executados remotamente em resposta à um incidente de segurança;

2.22.40. Deve permitir que o acesso remoto seja desabilitado globalmente em dispositivos específicos;

2.22.41. Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;

2.22.42. Deve permitir que administradores possam interromper tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento;

2.22.43. Possuir a capacidade de adição de endereços específicos para mesmo quando o dispositivo esteja em quarentena/contenção sejam alcançáveis, ou seja, quando houver o isolamento do dispositivo o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a console de gerência;

2.22.44. Deve permitir que proteção de dispositivos seja habilitada em modos de detecção somente, sem bloqueio efetivo;

2.22.45. Deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivo.

- a) Dispositivos de imagem;
- b) Dispositivos de áudio e vídeo;
- c) Dispositivos de armazenamento em massa;
- d) Dispositivos móveis (MTP/PTP);

- e) Impressoras;
- f) Adaptadores de rede wireless;
- g) Para dispositivos de armazenamento em massa, deve permitir acesso granular com no mínimo, as seguintes permissões:

- Leitura somente;
- Escrita e leitura;
- Escrita leitura e execução;
- Bloqueio total;

2.22.46. A proteção de dispositivos deve permitir exceções baseadas no Vendor ID e Product ID, número serial e classe;

2.22.47. Administração Firewall Local na mesma console;

- a) Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;
- b) A política de firewall deve permitir a utilização de múltiplas regras de firewall;
- c) As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;
- d) Regras de firewall devem suportar minimamente as seguintes características:
 - IPv4;
 - IPv6;
 - Protocolos:
 - Any;
 - TCP;
 - UDP;
 - ICMP;
 - Avançado (permitindo especificar o número do protocolo).
 - Endereço local;
 - Porta local;
 - Endereço remoto;
 - Porta remota;
 - Ação:
 - Permitir;

- Bloquear.
 - Direção da conexão:
 - Inbound;
 - Outbound;
 - Inbound ou Outbound.
- e) Perfil de rede (para que a regra seja aplicada de acordo com o perfil da interface de rede):
- Domínio;
 - Privado;
 - Público.
 - Processo;
- f) Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;
- g) As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente.

2.23. Características específicas para sistemas operacionais Linux

- a) Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção de ataques;
- b) Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;
- c) Deve permitir níveis de sensibilidade diferentes para detecção de ataques através do componente de aprendizado de máquina;
- d) Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
- e) Deve permitir bloqueio de processos com comportamento malicioso de acordo com a inteligência da fabricante.
- f) Deve permitir rodar comandos no dispositivo em tempo real por meio da console de gerenciamento em nuvem, precisando contemplar as seguintes ações:
- Mostrar as conexões de rede

- Mostrar os processos ativos
 - Encerrar um processo ativo
 - Reiniciar o dispositivo
 - Desligar o dispositivo
 - Acessar e deletar arquivos
- g) Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;
- h) Deve permitir que administradores possam interromper tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento.
- i) Possuir a capacidade de adição de endereços específicos para mesmo quando o dispositivo esteja em quarentena/contenção sejam alcançáveis, ou seja, quando houver o isolamento do dispositivo o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a console de gerência.
- j) Deve permitir monitorar atividade de arquivos de sistema para enriquecer a telemetria enviada a nuvem, melhorando a qualidade das detecções.
- k) Deve permitir monitorar atividade de rede para enriquecer a telemetria enviada a nuvem, melhorando a qualidade das detecções.

2.24. Capacidades de inteligência de ameaças

2.24.1. A inteligência de ameaças deve mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, país de origem da campanha e última atividade;

2.24.2. Para campanhas de ameaça, a inteligência de ameaças deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de entrega, breve descrição da campanha, forma de monetização, métodos de ataque e motivação da campanha.

2.24.3. Deve associar, quando pertinente, detecções presentes no ambiente à campanha de ataque;

2.24.4. Deve permitir extração de indicadores de comprometimento como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de email, nomes de arquivos associados às atividades maliciosas;

2.25. Capacidades de emulação de execução de código

2.25.1. A solução deve prover, integrada à console de administração, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros;

2.25.2. Deve se integrar ao agente instalado em dispositivos para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;

2.25.3. A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais:

- a) Windows 7 (32 e 64 bits);
- b) Windows 10;
- c) Linux Ubuntu;
- d) Android.

2.25.4. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

- a) Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK;
- b) Características comportamentais suspeitas;
- c) Imagens de execução, quando aplicável;
- d) Detalhes do arquivo como nome, hash, tamanho, tipo;
- e) Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- f) Atividades de arquivos;
- g) Detalhes de processos iniciados durante a execução.

2.26. Relatórios e dashboard.

2.26.1. A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.

2.26.2. A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada, como por exemplo por tática.

2.26.3. A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.

2.26.4. A plataforma deverá ter a capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros:

- a) Severidade;
- b) Tática;
- c) Técnica;
- d) Usuário;
- e) Host
- f) Tipo de sistema operacional;
- g) Versão do sistema operacional;
- h) Última hora;
- i) Último dia;
- j) Última semana;
- k) Últimos 30 dias
- l) Nome de arquivo;
- m) Hash do processo

2.26.5. A solução deve prover a capacidade de relatório de todas as conexões remotas realizadas desde a console de gerenciamento ao endpoint gerenciado contendo minimamente as seguintes informações que não deverão ser passíveis de exclusão ou limpeza, garantindo assim o não-repúdio:

- a) Login do administrador/operador que realizou a operação;
- b) Nome do endpoint.
- c) Duração da sessão.
- d) Data e hora do início da sessão;
- e) Arquivos copiados desde a máquina;
- f) Comandos executados na máquina;
- g) Data e hora de cada comando executado.

2.26.6. A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV:

- a) Hostname;
- b) Data e hora da primeira comunicação.
- c) Data e hora da última comunicação.
- d) Versão do sistema operacional;
- e) Modelo;
- f) Tipo;

- g) Unidade organizacional (OU);
- h) Site;
- i) Política de proteção aplicada;
- j) Política de resposta aplicada;
- k) Política de atualização aplicada;
- l) Política de controle de dispositivos USB aplicada;
- m) Identificação do host (UID/GUID);
- n) IP local da máquina;
- o) IP público da máquina;
- p) MAC Address;
- q) Versão do sensor/agente instalado.

2.26.7. O relatório de máquinas deverá ter a capacidade de aplicar filtros para inclusão ou exclusão de dados no relatório, considerando minimamente as seguintes opções de filtro:

- a) Domínio;
- b) Grupo;
- c) Identificação do host (UID/GUID);
- d) Hostname;
- e) IP local da máquina;
- f) MAC Address;
- g) Subnet da máquina;
- h) Versão do sistema operacional;
- i) Unidade organizacional (OU);
- j) Plataforma;
- k) Política de proteção aplicada;
- l) Política de resposta aplicada;
- m) Política de atualização aplicada;
- n) Versão do sensor/agente instalado.

2.26.8. Deverá apresentar a lista de dispositivos gerenciados com a capacidade de filtro baseado minimamente nas seguintes categorias;

- a) Por tipo do Sistema Operacional;
- b) Por versão do Sistema Operacional;

- c) Por plataforma do Sistema Operacional;
- d) Por unidade organizacional do host;
- e) Por nome do Site;
- f) Por Status do host;

2.27. Workflows e notificações

2.27.1. A solução deve possibilitar a criação de workflows de automatização para definir ações que o administrador quer que a solução execute em resposta a uma detecção, a uma política e uma atualização feita por um usuário.

2.27.2. Deve permitir a configuração dos seguintes gatilhos de início do workflow:

- a) Nova detecção
- b) Detecção atribuída a um usuário para investigação
- c) Política criada
- d) Política deletada
- e) Política habilitada
- f) Política desabilitada;
- g) Política atualizada.

2.27.3. Deve permitir a configuração das seguintes ações tomadas automaticamente

- a) Conter a rede do dispositivo, fazendo que ele só se comunique com a console da solução
- b) Pegue o arquivo associado a uma detecção da endpoint e faça o upload para a console
- c) Remova o arquivo associado a uma detecção do endpoint
- d) Notifique um usuário

2.27.4. A solução deve possibilitar a configuração dos seguintes canais de notificação no workflow:

- a) E-mail
- b) Microsoft Teams
- c) PagerDuty
- d) ServiceNow
- e) Slack
- f) Webhook

2.27.5. A solução deve possibilitar a configuração dos seguintes canais de notificação

no workflow:

- a) E-mail
- b) Microsoft Teams
- c) PagerDuty
- d) ServiceNow
- e) Slack
- f) Webhook

2. IMPLANTAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

2.1. Durante a etapa de implantação e migração, a solução fornecida pela CONTRATADA deverá ser colocada em plena operação, em condições reais de produção, e sua equipe deverá estar presente, nos horários de testes, implantação e migração, definidos pela ANTT, e estes horários poderão ser horário comercial, período noturno ou final de semana.

2.2. Compreende-se nesta etapa a instalação e configuração da solução e integração com os dispositivos necessários a serem protegidos, que deverá ser realizada em no máximo 15 (quinze) dias contados da data de assinatura do Contrato.

2.3. Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários e acessos necessários de acordo com as políticas e diretrizes de segurança da agência.

2.4. As atividades de instalação e configuração inicial da solução, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da ANTT.

2.5. A solução deverá ser instalada e configurada a integração com os dispositivos necessários a serem protegidos, em no máximo 15 (quinze) dias contados da data de assinatura do Contrato, e durante esta etapa, a equipe da CONTRATADA deverá estar de forma remota, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários necessários para os acessos necessários de acordo com as políticas e diretrizes de segurança da ANTT, sendo que as atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da equipe da ANTT e para esta ou qualquer outra

etapa a ANTT não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe acompanhará a ativação dos serviços, da console e a integração com os dispositivos, mantendo o alinhamento com ato PGJ 939/2019 da ANTT visando a transformação digital e seguindo a diretriz de fazer mais, melhor e com menos estrutura local.

3. DO SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA E TRANSFERÊNCIA DE CONHECIMENTO

3.1. Os atendimentos deverão ser do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, e deverá ser realizado por profissionais especializados, sendo necessário cobrir todo e qualquer defeito ou demanda apresentada.

3.1.1. Os serviços de suporte e manutenção consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e atualizações de versões para correções de eventuais problemas identificados.

3.1.2. As atividades de suporte técnico serão realizadas, a critério da ANTT, em seu ambiente, a partir da assinatura do Contrato e durante toda sua vigência contratual.

3.1.3. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração com os dispositivos da ANTT, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

3.1.3.1. Orientação sobre acesso, o uso, a configuração, a instalação da solução e a integração com os dispositivos da ANTT, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do FABRICANTE da solução.

3.1.3.2. Orientação quanto às melhores práticas para implementação e integração da solução no ambiente da ANTT.

3.1.3.3. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto nos agentes e/ou sensores já instalados no ambiente da ANTT.

3.1.3.4. Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas nos dispositivos protegidos e monitorados pela console central.

3.1.3.5. Aplicação de melhores práticas para implementação dos produtos de software adquiridos.

3.1.3.6. Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam.

3.1.3.7. Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas.

3.1.3.8. Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias novas integrações.

3.1.3.9. Identificação de melhorias e respectivo tratamento (melhoria de parametrização).

3.1.3.10. Parametrização da solução, de acordo com as regras e políticas disponíveis em sua console única e definidas pela ANTT.

3.1.3.11. Apoio para execução de procedimentos de atualização para novas versões dos agentes e/ou sensores instalados nos dispositivos

3.1.3.12. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário.

3.1.3.13. Suporte avançado para estratégia e planejamento de migrações e adequações nos agentes e sensores instalados nos dispositivos protegidos pela solução.

3.1.3.14. Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe da ANTT.

3.1.3.15. Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

3.1.3.16. A ANTT poderá solicitar durante toda a vigência contratual do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe, para isso serão abertos chamados com severidade “4”

classificado como “baixa”.

3.1.3.17. As transferências de conhecimento poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências da ANTT, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da ANTT, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução fornecida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

3.1.3.18. Serão solicitadas no mínimo, 2 (duas) workshops de transferência de conhecimento, sendo uma na implantação da solução, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente na ANTT e no máximo 1 (uma) workshop de transferência de conhecimento por mês caso a equipe da ANTT entenda que seja necessário.

3.1.3.19. Para os casos em que houver alguma mudança significativa que reflita na operação da solução ou reflita nos agentes e/ou sensores instalados nos dispositivos, a CONTRATADA deverá transferir este conhecimento para equipe interna da ANTT sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4”.

3.1.3.20. Os serviços de operação assistida poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverão ser realizados nas dependências da ANTT, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da SETUR, de modo que os trabalhos possam ser realizados com qualidade e eficácia, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

3.1.3.21. Será solicitado no mínimo, 1 (uma) sessão de operação assistida por trimestre, e no máximo 1 (uma) sessão por mês, devendo ocorrer logo após a implantação da solução, para possibilitar qualquer nova análise de funcionamento, configuração e/ou modificação necessárias nas implementações e integrações já realizadas, de modo que o funcionamento se mantenha sempre atualizado, em produção e devidamente funcional e integrado aos dispositivos pertencentes ao ambiente da ANTT.

3.1.4. O serviço deverá ocorrer durante toda a vigência contratual, e deverá ser disponibilizado pela CONTRATADA um sistema de acompanhamento e controle de chamados onde eles serão registrados com acesso liberado para cada integrante da equipe da ANTT que será informado no início da vigência contratual.

3.1.4.1. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe da ANTT.

3.1.4.2. Em casos de chamados abertos via telefone, o sistema deverá disponibilizar um número local onde a ANTT possui sua sede (Brasília, evitando custos desnecessários, onde o número deverá ser disponibilizado pela CONTRATADA no formato (061)+(número local) e deverá possibilitar a abertura de chamados por meio de gravação de áudio, caso os atendentes estejam ocupados no momento da ligação, devendo o sistema identificar o número utilizado pré-cadastrado e liberado para abertura de chamados que serão automaticamente abertos e enviados para uma fila de atendimentos apropriada, devendo registrar o horário do momento da ligação como horário de abertura do chamado em questão.

3.1.5. Os serviços serão prestados de forma remota observando as seguintes condições:

3.1.5.1. O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.

3.1.5.2. Durante as sessões remotas a CONTRATADA deverá utilizar ferramenta própria para acesso remoto seguro (exemplo: Bomgar, LogMeIn) ao ambiente da ANTT, possibilitando a gravação da sessão e possibilitando o acesso simultâneo de todos os envolvidos na solução do chamado, seguindo todas as diretrizes de segurança pré-estabelecidas.

3.1.5.3. Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Severidade	Descrição	Prazo máximo de início de atendimento remoto	Prazo máximo da solução
Urgente / Crítica Severidade 1	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após abertura do chamado remoto.
Alta Severidade 2	Impacto de alta significância relacionado à utilização do ambiente: ocorrência de indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias após abertura do chamado remoto.
Normal Severidade 3	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto.	Até 8 (oito) dias após abertura do chamado remoto.
Baixa Severidade 4	Consulta e/ou dúvida técnica e/ou transferência de conhecimento	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 10 (dez) dias após a abertura do chamado remoto.

3.1.6. Não haverá limite para o número de chamados de suporte técnico.

3.1.7. O nível de severidade será atribuído pela equipe autorizada da ANTT no momento da abertura do chamado.

3.1.8. Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que a ANTT estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de

protocolo/número de abertura do mesmo.

3.1.9. Uma vez que a solução estará em produção e funcionando em nuvem, as atividades relacionadas a correções ou atualizações da console que necessitarem indisponibilidade do ambiente, sem prejuízo para o funcionamento dos dispositivos já gerenciados pela solução, deverão ser notificadas a ANTT com antecedência mínima de 1 (um) dia útil.

3.1.10. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e caso seja definido pela ANTT poderão ser aplicadas glosas conforme tabela a seguir e serem descontadas da garantia financeira dos serviços prestados:

Resultado esperado e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
Crítica	1hora	$NHA * 0,7\% * VAS$	10% da VAS
Alta	1hora	$NHA * 0,5\% * VAS$	10% da VAS
Média	1hora	$NHA * 0,3\% * VAS$	10% da VAS

Onde:

NHA = Número de horas de atraso após o término do prazo máximo esperado para solução.

VAS = Valor anual da subscrição.

3.1.11. Durante o período de vigência do contrato a CONTRATADA deverá apresentar mensalmente relatório em formato eletrônico, contendo todos os chamados ocorridos no mês e seus prazos de atendimento, contendo informações analíticas e sintéticas de cada chamado, contendo a lista e total de chamados concluídos dentro e fora do prazo de SLA estabelecido.

3.1.12. Deverá ser garantido a ANTT pleno acesso as últimas atualizações e informações do FABRICANTE da solução, além de acesso irrestrito a solução, sendo obrigação da CONTRATADA a abertura de qualquer chamado necessário junto a equipe de suporte do FABRICANTE, caso seja necessário, devendo possuir todos os acessos necessários para a execução dos serviços de suporte técnico com a operação assistida e transferência de conhecimento.

----- FIM DO APÊNDICE "A" -----