GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

ANÁLISE

Análise nº 16/2024/IPERON-DTIC

De: IPERON-DTIC

Para: IPERON-EQCOM

Processo Nº: 0016.000487/2024-37

Senhora Pregoeira,

Em atenção ao despacho SUPEL ID 0053382103 qual dispõe sobre a análise da proposta, das empresas **MICROHARD INFORMATICA LTDA** (0053379049) , **SOFTWARESULTEK TECNOLOGIA DA INFO** (0053379713) e **IMAGETECH TECNOLOGIA EM INFORMATI** (0053380211) , vendedoras do lote 1 decorrentes ao PREGÃO ELETRÔNICO Nº 90285/2024/SUPEL/RO**,** conforme **características e exigências os objetos do** Instrumento Convocatório ID 0051303047 e Termo de Referência (ID 0052488109) . Temos as seguintes considerações:

1. DAS PROPOSTAS DE PREÇO

1.1. Proposta - **MICROHARD INFORMATICA LTDA** (0053379049)

Lote 1 - Aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações.

Item	Descrição	Marca / Modelo	Unidade	Quantidade	Valor Unitário	Valor Total
1	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (trinta e seis) meses**	Kaspersky Next EDR Optimum Brazilian Edition	Licença	400	R$294,00	R$117.600,00
2	**Serviço de treinamento** da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos.	Microhard	Turma	1	R$10.000,00	R$10.000,00

TOTAL DA PROPOSTA: R$127.600,00 (cento e vinte e sete mil e seiscentos reais)

1.2. Proposta - **SOFTWARESULTEK TECNOLOGIA DA INFO** (0053379713)

Lote 1 - Aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações.

Item	Descrição	Marca / Modelo	Unidade	Quantidade	Valor Unitário	Valor Total
1	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (trinta e seis) meses**	Kaspersky Next EDR Optimum Brazilian Edition	Licença	400	R$323,00	R$129.200,00
2	**Serviço de treinamento** da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos.	SOFTWARESULTEK	Turma	1	R$ 11.700,00	R$ 11.700,00
	TOTAL DA PROPOSTA: R$ 140.900,00 (cento e quarenta mil e novecentos reais)					

1.3. Proposta - **IMAGETECH TECNOLOGIA EM INFORMATI** (0053380211)

Lote 1 - Aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações.

Item	Descrição	Marca / Modelo	Unidade	Quantidade	Valor Unitário	Valor Total
1	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (trinta e seis) meses**	Kaspersky Next EDR Optimum Brazilian Edition	Licença	400	Rs 333,10	R$ 133.240,00

2	**Serviço de treinamento** da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos.	IMAGETECH	Turma	1	R$ 10.079,57	Rs 10.079,57
	TOTAL DA PROPOSTA: R$ 143.319,57 (cento e quarenta e três mil trezentos e dezenove reais e cinquenta e sete centavos)					

1.4.

2. DOS REQUISITOS PARA ACEITAÇÃO DA PROPOSTA

2.1. Considerando item 6 do instrumento convocatório ID 0052114038:

> 6.2. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos: Valor unitário e total do item ou valor global, ou percentual de desconto; descrição detalhada do objeto, contendo as informações conforme à especificação do Termo de Referência.
>
> 6.3. Nos valores propostos estarão **inclusos todos os custos operacionais**, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.
>
> 6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
>
> 6.5. As ofertas de propostas dos licitantes devem respeitar os preços máximos estabelecidos neste Edital.
>
> 6.6. As propostas terão validade mínima de 90 (noventa) dias, a contar da data de sua apresentação.

2.2. **DAS ESPECIFICAÇÕES QUE COMPÕE A SOLUÇÃO:**

TERMO DE REFERÊNCIA	**MICROHARD INFORMATICA LTDA** (0053379049)	**SOFTWARESULTEK TECNOLOGIA DA INFO** (0053379713)	**IMAGETECH TECNOLOGIA EM INFORMATI** (0053380211
ITEM 01 - Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por 36 (trinta e seis) meses **Requisitos Gerais:** Subscrição de proteção de endpoints, com implementação e suporte técnico por **36 (Trinta e Seis) meses**, incluindo treinamento para turma de alunos. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças: Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing,			

vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI). A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender. A solução proposta deve suportar o subsistema Linux no Windows. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo: Proteção contra ameaças sem arquivos (Fileless); Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque; A solução proposta deve fornecer varredura de memória para estações de trabalho Windows; A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para				

estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows. A solução proposta deve fornecer análise comportamental baseada em machine learning. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint: Controles de aplicativos, Controle web e dispositivos HIPS e Firewall Descoberta de patches e vulnerabilidades de sistemas operacionais Windows; Gerenciamento de criptografia de arquivos e discos; Controle adaptativo para detecção de anomalias; A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema. A solução proposta deve ter bancos de dados de reputação locais e globais. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares. A solução proposta deve incluir um módulo capaz, no mínimo, de: Bloqueio de aplicativos com base em sua categorização. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.				

A adição de sub-redes e a modificação de permissões de atividade. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades: Modo silencioso; Discos rígidos e dispositivos removíveis; De todos as contas de usuários do dispositivo. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos: Exclusão imediata de dados; Exclusão de dados adiada. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados: Excluir usando os recursos do sistema operacional - os arquivos são excluídos; Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção				

contra ações maliciosas. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint; A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho; A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint. A solução proposta deve suportar detecção baseadas em multicamadas				

sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo. A solução proposta deve ter categoria de detecção para bloquear banners de sites. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis; A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos. A solução proposta deve apresentar				

integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo; A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões. A solução proposta deve suportar o controle de scripts executados em PowerShell. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em				

nuvem. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com: Filtro de anexos. Verificação de mensagens de email ao receber, ler e enviar. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo; A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.); A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de				

computadores de qualquer tipo, incluindo redes sem fio. A solução proposta deve incluir suporte ao protocolo IPv6. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação: Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados. A solução proposta deve, ao detectar atividades semelhantes a				

ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição. A solução proposta deve suportar endereços IPv6. A solução proposta deve suportar verificação em duas etapas (autenticação). A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes. A solução proposta deve permitir a atualização automática do sensor de				

endpoint e de bases de dados de anti-malware. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos. A solução proposta deve ter a capacidade de excluir atualizações baixadas. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.				

A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo: Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados. A solução proposta deve gerar relatorios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado. **Do Módulo de proteção de endpoint:**				

A solução proposta deverá proteger os sistemas operacionais abaixo: Windows 7 Windows 8 Windows 8.1 Windows 10 Windows 11 Windows Small Business Server 2011 Windows MultiPoint Server 2011 Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 Servidores de terminal Microsoft Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 Sistemas operacionais Linux de 32 bits: CentOS 6.7 e posterior Debian GNU/Linux 11.0 e posterior Debian GNU/Linux 12.0 e posterior Red Hat Enterprise Linux 6.7 e posterior Amazon Linux 2. CentOS 6.7 e mais tarde CentOS 7.2 e posterior. CentOS Stream 8. CentOS Stream 9. Debian GNU/Linux 11.0 e posterior. Debian GNU/Linux 12.0 e posterior. Linux Mint 20.3 e superior. Linux Mint 21.1 e posterior. openSUSE Leap 15.0 e posterior. Oracle Linux 7.3 e posterior. Oracle Linux 8.0 e posterior. Oracle Linux 9.0 e posterior. Red Hat Enterprise Linux 6.7 e posterior Red Hat Enterprise Linux 7.2 e posterior. Red Hat Enterprise Linux 8.0 e posterior.				

Red Hat Enterprise Linux 9.0 e posterior. Rocky Linux 8.5 e posterior. Rocky Linux 9.1. SUSE Linux Enterprise Server 12.5 ou posterior. SUSE Linux Enterprise Server 15 ou posterior. Ubuntu 20.04 LTS. Ubuntu 22.04 LTS. CentOS Stream 9. SUSE Linux Enterprise Server 15. Ubuntu 22.04 LTS. macOS 12 – 14 Ferramentas de virtualização MAC OS: Parallels Desktop 16 para Mac Business Edition VMware Fusion 11.5 Profissional VMware Fusion 12 Profissional A solução proposta deverá suportar as seguintes plataformas virtuais: VMware Workstation 17.0.2 Pro VMware ESXi 8.0 Update 2 Microsoft Hyper-V Server 2019 Citrix Virtual Apps e Desktop 7 2308 Citrix Provisioning 2308 Citrix Hypervisor 8.2 Update 1 **Do Módulo de Gerenciamento Avançado:** A solução proposta deve suportar arquitetura cloud-native e on-premisse; A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de: Amazon Web Services; Microsoft Azure; A solução proposta deve incluir as seguintes opções de integração SIEM: HP (Microfoco) ArcSight; IBM QRadar; Splunk;				

Kaspersky KUMA; A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes; A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas; A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos; O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede; A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador; A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento; A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização; A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis; O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem; O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos				

perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação: Status do dispositivo; Tag; Diretório ativo; Proprietários de dispositivos; Hardware; A solução proposta deve suportar os seguintes canais de entrega de notificação: E-mail; Registro de sistema; SMS; A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em: Atributos de rede; Nome; Domínio e/ou Sufixo de Domínio; Endereço de IP; Endereço IP para servidor de gerenciamento; Localização no Active Directory; Unidade organizacional; Grupo; Sistema operacional; Número do pacote de serviço; Arquitetura Virtual; Registro de aplicativos; Nome da Aplicação; Versão do aplicativo; Fabricante; Tipo e versão; Arquitetura; A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão;				

A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública; As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte: Dispositivos Desktop/Servidores Dispositivos móveis; Dispositivos de rede; Dispositivos virtuais; Componentes OEM; Periféricos de computador; Dispositivos IoT conectados; Telefones VoIP; Repositórios de rede; A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em: Nome da Aplicação; Caminho do aplicativo; Metadados do aplicativo; Aplicativo Certificado digital; Categorias de aplicativos predefinidas pelo fornecedor; SHA256 e MD5; A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos: Bluetooth; Dispositivos móveis; Modems externos; CD/DVD; Câmeras e scanners; MTPs; E a transferência de dados para dispositivos móveis; A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na				

organização; A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão; A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados: Estruturas de domínios e grupos de trabalho do Windows; Estruturas de grupos do Active Directory; Conteúdo de um arquivo de texto criado manualmente pelo administrador; A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização. A solução proposta deve permitir realizar as seguintes ações para endpoints: Verificação manual; Verificação no acesso; Verificação por demanda; Verificação de arquivos compactados Verificação de arquivos individuais, pastas e unidades; Bloqueio e verificação de scripts Proteção contra alteração de registros; Proteção contra estouro de buffer; Verificação em segundo plano/inativa. Verificação de unidade removível na conexão com o sistema; A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.				

O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração. A solução proposta deve suportar Windows Failover Cluster. A solução proposta deve ter um recurso de clustering integrado. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux. A solução proposta deve ser capaz de				

registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes. A solução proposta deverá possuir controles para download de DLL e drivers. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log). A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.				

A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo	**Kaspersky Next EDR Optimum Brazilian Edition**	**Kaspersky Next EDR Optimum Brazilian Edition**	**Kaspersky Next EDR Optimum Brazilian Edition**

selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. . A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis. A solução proposta deve permitir ao administrador personalizar relatórios. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico. A funcionalidade 'Dispositivo				

desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos; O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários. A solução proposta deve suportar integração com solução APT. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais: Windows; Linux; A solução proposta deverá suportar os seguintes servidores de banco de dados: Microsoft SQL Server; Microsoft Banco de dados SQL do Azure; MySQL Standard e Enterprise; MariaDB; PostgreSQL; MySQL; MariaDB; PostgreSQL; A solução proposta deverá suportar as seguintes plataformas virtuais: VMware vSphere 6.7 e 7.0; Estação de trabalho VMware 16 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits;				

Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Oracle VM VirtualBox 6.x; VMware vSphere 6.7, 7.0 e 8.0; VMware Desktop 16 Pro e 17 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 e 8.x; Oracle VM VirtualBox 6.x e7.x; A solução proposta deve suportar criptografia em vários níveis: Criptografia completa do disco – incluindo disco do sistema; Criptografia de arquivos e pastas; Criptografia de mídia removível; Gerenciamento de criptografia BitLocker e MacOS Filevault2; A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita: A criptografia de arquivos em unidades de computador locais; A criação de listas de criptografia de arquivos por extensão ou grupo de extensões; A criação de listas criptografadas de pastas em unidades de computador locais; A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE)				

que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de: Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis; Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais; A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis: A criptografia de todos os arquivos armazenados em unidades removíveis; A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis; A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado. A solução proposta deve oferecer a				

capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-				

passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo: Uso do Trusted Platform Module e configurações de senha; Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível; Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets); A solução proposta deve suportar criptografia em Microsoft Surface Tablets; A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo: Instalação remota de software de terceiros; Relatórios sobre software e hardware existentes; Monitoramento para instalação de software não autorizado; Remoção de software não autorizado; A solução proposta deverá incluir				

recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança A solução proposta deve permitir ao administrador aprovar atualizações. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem				

disponíveis. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências). A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade". A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes. A solução proposta deve apoiar a implantação do sistema operacional. A solução proposta deve suportar Wake-on LAN e UEFI. A solução proposta deve ter funcionalidade integrada de				

compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros: Inicie a instalação ao reiniciar ou desligar o computador; Instale o gerador necessário todos os				

pré-requisitos do sistema; Permitir a instalação de novas versões de aplicativos durante as atualizações; Baixe atualizações para o dispositivo sem instalá-las; A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos: CEF; LEEF; A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais. O relatório da solução proposta deve conter informações CVE. A solução proposta deve suportar instalação de aplicações e software de terceiros; **Do Módulo de Gerenciamento Simplificado:** A solução proposta deve suportar arquitetura cloud; A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.				

A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint. A solução proposta deve atender as condições apontadas no item e subintes 6. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS. A solução proposta deve incluir informações do endpoint: IP público de internet; IP interno do dispositivo; Versão do agente de proteção; Ultima comunicação com a console, contendo data e hora; Informações do sistema operacional; A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365. A solução proposta deve incluir treinamento em segurança cibernética. **Do Módulo de Gerenciamento de Dispositivos Móveis:** O modulo deve ser integrado a console de gerenciamento; A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android: Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition) A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS: iOS 10–17 ou iPadOS 13–17 A solução proposta deve oferecer suporte a dispositivos Android Device Owner.				

A solução proposta deve suportar dispositivos iOS supervisionados. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais). A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado. A solução proposta deve ter recursos de conteinerização para dispositivos Android. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android: Dados em contêineres Contas de e-mail corporativo				

Configurações para conexão à rede Wi-Fi corporativa e VPN Nome do ponto de acesso (APN) Perfil do Android for Work Recipiente KNOX Chave do gerenciador de licença KNOX A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS: Todos os perfis de configuração instalados Todos os perfis de provisionamento O perfil iOS MDM Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo . A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes: Critérios de verificação do dispositivo; Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido; A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:				

Cartões de memória e outras unidades removíveis Câmera do dispositivo Conexões Wi-Fi Conexões Bluetooth Porta de conexão infravermelha Ativação do ponto de acesso Wi-Fi Conexão de área de trabalho remota Sincronização de área de trabalho Definir configurações da caixa de correio do Exchange Configurar caixa de e-mail em dispositivos iOS MDM Configure contêineres Samsung KNOX. Definir as configurações do perfil do Android for Work Configurar e-mail/calendário/contatos Defina as configurações de restrição de conteúdo de mídia. Definir configurações de proxy no dispositivo móvel Configurar certificados e SCEP A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay . A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel: Google Play, Huawei App Gallery e Apple App Store Portal de inscrição móvel KNOX Pacotes de instalação pré-configurados independentes A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.				

A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros: VMware AirWatch 9.3 ou posterior MobileIron 10.0 ou posterior IBM MaaS360 10.68 ou posterior Microsoft Intune 1908 ou posterior SOTI MobiControl 14.1.4 (1693) ou posterior A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de: Google Play Galeria de aplicativos Huawei Loja de aplicativos da Apple A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console				

usado para gerenciar computadores e servidores. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes; A solução proposta deve proteger contra ameaças online em dispositivos iOS. **Do Módulo de EDR:** Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças; Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise; Deve apresentar informações				

detalhadas contendo: Usuário que executou a ação; Informações acesso privilegiado; A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas. A solução proposta deve suportar integração com serviço de reputação em nuvem. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.) O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único). Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas; A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.				

A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada: Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque). Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional. Informações gerais sobre a detecção, incluindo modo de detecção. Alterações no registro associadas à detecção. Histórico da presença de arquivos no dispositivo. Ações de resposta executadas pela aplicação. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:				

Processo Conexões de rede Alterações no registro Detalhes do download de objeto A solução proposta deve fornecer orientação de resposta (resposta guiada). A solução proposta deve suportar "clique único" no console de gerenciamento avançado para resposta a um incidente A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas: Impedir a execução de objetos Isolamento de host Excluir objeto do host ou grupo de hosts Encerrar um processo no dispositivo Colocar um objeto em quarentena Execute a verificação do sistema Execução remota de programa/processo/comando Iniciar a varredura IoC para um grupo de hosts. **Requisitos de Documentação:** A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos: Ajuda on-line para administradores Ajuda on-line para melhores práticas de implementação Ajuda on-line para proteção de servidores de administração A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware. Deve estar disponível página com informações de ciclo de vida das soluções e módulos; **Requisitos do Treinamento:** A licitante deverá realizar treinamento				

da solução ofertada, com carga horária mínima de 16 (Dezesseis) horas de duração, para turma de no mínimo 3 (Três) alunos. O treinamento deverá ser realizado em dias úteis, em horário de funcionamento do Iperon das 7:30 as 13:30 (Horário local) O treinamento pode ser realizado de forma remota (Online). Deverá ser emitido certificado de participação ao final do curso para cada participante. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato. Deverá ser abordado em seu conteúdo programático, no mínimo, os seguintes temas: Solução de Antivírus, Firewall; Controle de Aplicativos; Controle de Acesso à WEB; Controle de Dispositivos (USB); Gerenciamento de vulnerabilidades e correções; Console de Gerenciamento Integrada. **Requisitos Gerais para a Segurança da Contratação:** Caso não seja o próprio fabricante, o licitante deverá apresentar Carta do Fabricante específica para este certame, juntamente com a proposta comercial comprovando ser revenda autorizada, certificada e habilitada para fornecer a subscrição destes softwares, bem como prestar serviços de suporte técnico especializado, realizar treinamentos, instalação e configuração. O licitante deverá apresentar, juntamente com a proposta comercial, documentação de vínculo empregatício de até 2 (dois) profissionais técnicos juntamente com os respectivos certificados, sendo estes profissionais aptos a prestar o serviço de suporte técnico que for necessário. O licitante vencedor desta licitação, deverá apresentar juntamente com a			

proposta comercial, certificação de boas práticas ITIL Foundation, de pelo menos um profissional que será responsável por ser o ponto de referência das demandas técnicas desta instituição, durante todo o período de garantia da subscrição deste software. Deverá ser anexada na proposta comercial a comprovação de certificação do profissional, no produto fornecido.			

ITEM 02 - Serviço de treinamento da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos. 2.3. **Requisitos do Treinamento:** A licitante deverá realizar treinamento da solução ofertada, com carga horária mínima de 16 (Dezesseis) horas de duração, para turma de no mínimo 3 (Três) alunos. O treinamento deverá ser realizado em dias úteis, em horário de funcionamento do Iperon das 7:30 as 13:30 (Horário local) O treinamento pode ser realizado de forma remota (Online). Deverá ser emitido certificado de participação ao final do curso para cada participante. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato. Deverá ser abordado em seu conteúdo programático, no mínimo, os seguintes temas: Solução de Antivírus, Firewall; Controle de Aplicativos; Controle de Acesso à WEB; Controle de Dispositivos (USB); Gerenciamento de vulnerabilidades e correções; Console de Gerenciamento Integrada.	**Microhard**	**SOFTWARESULTEK**	**IMAGETECH**

2.4. **CRITÉRIO DE JULGAMENTO DAS PROPOSTAS:**

O julgamento da Proposta de Preços dar-se-á pelo critério de MENOR PREÇO GLOBAL, observadas as especificações técnicas e os parâmetros mínimos de desempenho definidos neste Instrumento, em conformidade com a Lei Federal n. 14.133/21 e suas alterações.

Na proposta deverá constar o preço unitário e total, expressos em moeda corrente nacional, nele incluídas todas as despesas com a confecção, impostos, taxas, seguro, frete e embalagem, depreciação, emolumentos e quaisquer outros custos que, direta ou indiretamente venha ocorrer.

3. DA ANALISE DAS PROPOSTA

3.1. Após análise das propostas apresentadas pelas empresas **MICROHARD INFORMATICA LTDA** (CNPJ: 00.533.790/49), **SOFTWARESULTEK TECNOLOGIA DA INFO** (CNPJ:

00.533.797/13) e **IMAGETECH TECNOLOGIA EM INFORMATI** (CNPJ: 00.533.802/11), temos os seguintes apontamentos:

3.2. **MICROHARD INFORMATICA LTDA** (CNPJ: 00.533.790/49): Atende todos os itens do termo de referência;

3.3. **SOFTWARESULTEK TECNOLOGIA DA INFO** (CNPJ: 00.533.797/13): Atende quantos as especificações da solução apresentada, no caso o software **Kaspersky Next EDR Optimum Brazilian Edition.** No entanto não apresentou declaração **do fabricante nem dos 2 (dois) profissionais técnicos** conforme descrito no item 6.9 e subitens do Termo de referência ID 0052488109. Caso a empresa seja selecionada, será necessário a apresentação da documentação citada para prosseguimento na contratação.

3.4. **IMAGETECH TECNOLOGIA EM INFORMATI** (CNPJ: 00.533.802/11): Atende quantos as especificações da solução apresentada, no caso o software **Kaspersky Next EDR Optimum Brazilian Edition.** No entanto não apresentou declaração **do fabricante** conforme descrito no item 6.9 e subitens do Termo de referência ID 0052488109. Caso a empresa seja selecionada, será necessário a apresentação da documentação citada para prosseguimento na contratação.

4. DA CONCLUSÃO

4.1. Com base na análise técnica das propostas, constatamos que a empresa **MICROHARD INFORMATICA LTDA** está plenamente apta para prosseguimento da contratação**.**

4.2. Quanto à empresas **SOFTWARESULTEK TECNOLOGIA DA INFO** e **IMAGETECH TECNOLOGIA EM INFORMATI**, caso forem selecionadas, precisam apresentar a documentação necessária, conforme item 6.9 e subitens do Termo de referência ID 0052488109.

Elaborado por:

GABRIEL VAZ SEVERO

Analista de sistemas - Assessor

Revisado por

EZEQUIEL NASCIMENTO DA SILVA
Assessor

Aprovador por:

RUDNY WALLAS ALVES
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Gabriel Vaz Severo**, **Analista**, em 04/10/2024, às 12:41, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **EZEQUIEL NASCIMENTO DA SILVA** , **Assessor(a)**, em 04/10/2024, às 13:00, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Rudny Wallas Alves**, **Diretor(a)**, em 04/10/2024, às 13:11, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0053422999** e o código CRC **55E0D85B**.

Referência: Caso responda esta Análise, indicar expressamente o Processo nº 0016.000487/2024-37 SEI nº 0053422999