PREFEITURA DE
XANXERÊ

TERMO DE REFERÊNCIA

Unidade Requisitante: Secretaria de Administração e Finanças

Ordenador da despesa: Adenilso Biasus

(01) Objeto: Aquisição de software antivírus next antivírus generation de 140 (cento e quarenta) licenças de uso e atualização por 36 (trinta e seis) meses, sendo 15 (quinze) software para Windows server 2008/2012/2016 e o restante em estações Windows 7/8/10.

(02) Motivação/Justificativa

A pretendida contratação faz-se indispensável, pois visa prover segurança, proteção e automação do monitoramento da rede da Prefeitura de Xanxerê e de suas respectivas unidades, de forma a minimizar e, em grande parte, coibir a contaminação dos serviços e sistemas informatizados por programas ou atividades digitais maliciosas, contribuindo para a garantia do nível mínimo adequado e desejado de proteção dos dados e informações do Município.
A aquisição da solução de antivírus centralizada permitirá que as áreas responsáveis pela administração dos recursos de Infraestrutura de Tecnologia da Informação do Município de Xanxerê mantenham os níveis exigidos de segurança das informações trafegadas em rede e os controles e políticas necessárias para certificar que tais informações estão sendo acessadas e manipuladas somente por pessoas autorizadas. Tal fato resulta em otimização da infraestrutura de segurança dos dados armazenados na instituição e, também, provê serviços com confidencialidade para as informações trafegadas e armazenadas nas estações de trabalho e nos mais diversos sistemas corporativos do Município e suas unidades.

(03) Especificações técnicas:

Funcionalidades Básicas Antimalware (Windows, Linux, MacOS)
As funcionalidades listadas nesta seção devem estar disponíveis em todas as seguintes plataformas:
Microsoft Windows Endpoint
Windows 10
Windows 8.1
Windows 7
Microsoft Windows Server
Windows Server 2019
Windows Server 2016
Windows Server 2012 e 2012 R2
MacOS
Catalina 10.15.x
Mojave 10.14.x
High Sierra 10.13.x
Sierra 10.12.x
El Capitan 10.11.x
Linux
CentOS 6, 7 e 8
Debian 8 e 9
Fedora 22 a 30

OpenSUSE
Oracle Enterprise Linux 6 e 7
RedHat Enterprise Linux Server 6, 7 e 8
SUSE Linux Enterprise Server 11, 12 e 15
SUSE Linux Desktop 11 e 12
Ubuntu 17, 18 e 19
Toda a solução deverá funcionar com apenas um único agente instalado na estação de trabalho/servidor;
O agente deverá ser o responsável por toda a comunicação entre o cliente gerenciado (estação de trabalho/servidor) e o servidor de gerenciamento central e realizar as seguintes operações:
Instalar produtos e suas atualizações nos clientes gerenciados;
Instalar atualizações de assinaturas;
Garantir a execução das políticas definidas via console de gerenciamento central;
Executar tarefas conforme definidas via console de gerenciamento central;
Coletar informações e eventos do cliente gerenciado e enviá-las para a console de gerenciamento central;
O agente deve fazer o download apenas das mudanças realizadas nas suas políticas, consumindo menos recursos de processamento e de rede;
A comunicação entre o cliente gerenciado e o servidor de gerenciamento central deverá autenticado por um par de chaves para garantir a identidade das partes;
O agente deve ser capaz de realizar múltiplas operações de envio e recebimento de informações (ex: download de políticas e upload de eventos) em uma única conexão TCP, para menor consumo de recursos de rede;
O agente deve ser capaz de detectar o usuário que está "logado" no sistema para aplicar corretamente as políticas baseadas em usuários (user-based policies);
Deve ser possível realizar a atualização de assinaturas e engines através de comunicação peertopeer entre clientes gerenciados de uma mesma rede local, reduzindo o consumo de banda para o servidor de gerenciamento;
O agente deve possuir mecanismos próprios de proteção de seus dados, arquivos, pastas e registros (self protection);
O agente deve enviar para o servidor de gerenciamento central informações sobre o cliente gerenciado incluindo, pelo menos, as seguintes:
Endereço MAC, IP, Endereço da Subrede e Máscara
Nome de DNS e Domínio
Sistema Operacional, tipo e versão
Produtos da solução antimalware instalados no sistema
Espaço em disco total, livre e utilizado
Memória física total e memória livre
Uso do Processador
Nome ou Login do usuário
A solução deve possuir mecanismo baseado em assinaturas para detecção de malware.
A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos;
As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução;
O mecanismo de assinaturas deve ser acionado em tempo real, no momento de acesso aos arquivos e por comando do usuário/administrador de maneira agendada.
Ao detectar código malicioso, a solução deve executar ações e enviar alerta ao administrador;
Deve possuir pelo menos as seguintes ações primárias para arquivos infectados:
Negar acesso ao arquivo
Remover o arquivo

Limpar o arquivo
Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real e em varreduras agendadas);
Permitir incluir ou excluir pastas de rede e arquivos compactados das varreduras;
Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com horários determinados, de forma a reduzir impacto em ambientes;
Não serão aceitas soluções de Antimalware que possuam engine de terceiros;
A solução deve permitir a definição de repositórios distribuídos que contenham atualizações de assinaturas, engines, software e patches a serem instalado nos clientes gerenciados, de forma a reduzir o consumo de banda e a sobrecarga de conexões a um único repositório centralizado;
O repositório principal (master) deve concentrar o download das atualizações a partir do site do fabricante e distribuir a informação para os demais repositórios:
Automaticamente quando novos pacotes são atualizados no repositório principal;
De forma agendada;
De forma manual, sob demanda do administrador.
Além de solução de repositório distribuído do próprio fabricante, a solução deve permitir ainda a definição de repositórios distribuídos acessíveis através de HTTP e compartilhamento de pastas de rede;
Deve ser possível criar uma hierarquia de repositórios distribuídos de tal forma que um repositório distribuído seja a fonte de dados para outros repositórios, reduzindo o tráfego de rede;
Deve ser possível ao administrador definir as fontes de atualização dos arquivos de assinatura, software, novas engines de scaneamento para cada cliente/grupo de clientes gerenciados:
Deve ser possível impedir que os agentes busquem atualizações diretamente no repositório central, reduzindo a carga sobre o mesmo;
Deve ser possível definir uma lista ordenada de repositórios para que o cliente gerenciado busque as informações atualizadas.
A solução deve permitir a automação do processo de testes das novas assinaturas e engines disponibilizadas pelo fabricante, aplicando-as de forma automática em um grupo de máquinas de teste;
A distribuição das novas assinaturas e engines para o restante dos clientes gerenciados deve poder ser realizada de forma automática, em horário determinado, e também manualmente pelo administrador;
A solução deve permitir retornar as atualizações de engines e assinaturas à versão imediatamente anterior à versão corrente.
Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função;
Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução;
A solução deve prover mecanismos escalabilidade, fail-over e balanceamento de carga para acesso e distribuição das informações do repositório central;
A solução deve prover mecanismos para gerenciamento de clientes (ex: iniciar uma tarefa imediatamente) que estejam em redes com tradução de endereços (NAT), tais como Rede DMZ e Rede Interna de unidade que usa Firewall/NAT.
Cliente Gerenciado
O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede;
O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento;

Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante;
Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária;

Funcionalidades de Firewall e de Prevenção de Intrusão Para Plataforma Windows Endpoints
A solução deve permitir habilitar/desabilitar o módulo de firewall.
Deve permitir criar regras de bloqueio/liberação por aplicação/serviço.
Deve permitir o agrupamento de regras para facilitar o gerenciamento.
Deve permitir o agendamento das regras (schedule).
Deve possuir opção de Firewall de DNS impedindo a resolução de endereços para domínios definidos pelo administrador.
Deve permitir a criação de regras baseadas em camada 2 (Redes com Fio, Redes sem Fio, VPN's).
Deve permitir a criação de regras na camada de endereçamento IP, com suporte e IPV4 e IPV6.
Deve permitir a criação de regras baseadas no protocolo da camada de transporte (TCP, UDP, ICMP).
Deve possuir opção de bloquear ou liberar protocolos não conhecidos.
Deve permitir a criação de grupos de regras baseados em condições de localização de forma que um equipamento com múltiplas interfaces de rede possa ter políticas diferenciadas para cada interface.
As condições de localização dos grupos de regras devem incluir pelo menos os seguintes:
Sufixo de DNS da conexão
Gateway IP
DHCP IP
DNS server
WINS server
Endereço IP Local
Deve permitir o isolamento de conexões de forma a bloquear tráfego por interfaces alternativas, tais como usuários conectados à rede corporativa e com conexão sem fio a um provedor desconhecido. Neste caso, todo tráfego para a conexão sem fio deve ser bloqueado enquanto a máquina estiver conectada na rede corporativa.
Deve possuir catálogo de objetos pré-definidos para utilização nas regras de firewall/IPS e deve permitir a criação de novos objetos.
O catálogo deve incluir pelo menos os seguintes tipos de objetos:
Grupos - Listas de grupos de firewall e propriedades
Regras - Listas de regras de firewall e propriedades
Aplicações - Listas de aplicações que podem ser referenciadas em um grupo ou regra de firewall
Executáveis - Listas de executáveis vinculados às aplicações que podem ser referenciados em grupos/regras de firewall ou aplicações relacionadas ao HIPS
Redes - Listas de endereços IP que podem ser referenciadas em um grupo ou regra de firewall
O módulo de firewall deve realizar filtragem e inspeção de pacotes em modo stateful.
Deve ser possível a criação de políticas de firewall por usuário, quando integrado a um servidor LDAP.
A inspeção de pacotes deve funcionar em camada 7, analisando o tráfego da aplicação com verificações específicas para os protocolos de FTP, DNS e DHCP.
Deve possuir modo de funcionamento do tipo "learning", onde o sistema questiona os usuários sobre a liberação ou não de determinados tipos de conexão, e do tipo "adaptative", onde as regras são criadas automaticamente pelo sistema de acordo com tráfego normal do usuário.
Deve possuir opção de impedir todo o tráfego de entrada até que o módulo de IPS esteja ativo.
Deve possuir proteção contra IP Spoofing

Deve permitir a utilização de reputação de IP, provida pelo fabricante, para bloquear conexões de entrada.
Deve permitir a utilização de reputação de IP, provida pelo fabricante, para bloquear conexões de saída.
Deve permitir a definição de timeout para conexões TCP (modo stateful firewall)
Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;
Deve possuir o recurso de blindagem, impedindo o comprometimento dos aplicativos e dos seus dados, além de evitar que um aplicativo seja usado para atacar outros aplicativos;
Possuir proteção completa, pronta para operação e contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-dayattacks);
Capacidade de trabalhar no modo adaptativo se adaptando a novas aplicações instaladas na máquina;
Permitir o bloqueio de ataques baseados em Web como: DirectoryTraversalAttacks e Unicode Attacks;
Interceptar tráfego e requisições de HTTP após decriptação e decodificação;
Capacidade de detectar e bloquear tentativas de invasão;
Permitir monitoração de Hooking de aplicações com opções de permitir ou bloquear o hooking para uma lista de processos.
Permitir criar regras de bloqueio/permissão utilizando protocolos ou aplicações;
Permitir configuração de regras de firewall por horários (schedule).
Ser possível criar regras de tráfego de rede de maneira automática;
Ser possível configurar liberações de portas de maneira automática para aplicações confiáveis;

Funcionalidades de Controle de Dispositivos Para Plataforma Windows Endpoints
Deve ser capaz de controlar dispositivos externos conectados às máquinas corporativas tais como smartphones, dispositivos de armazenamento removíveis, dispositivos Bluetooth, MP3 players e dispositivos plug-and-play;
Deve ser possível definir padrões de dispositivos a partir de propriedades comuns como, pelo menos, bus type (Bluetooth, Firewire IEEE1394, IDE/SATA, PCI, PCMIA, SCSI, USB), device class, vendor ID, product ID, File System Type (CDFS, exFAT, FAT16, FAT32, NTFS, UDFS) e III. USB Device Serial Number
Deve ser possível agrupar padrões de dispositivos e definir regras aplicáveis a estes grupos;
Deve ser possível definir a quais usuários cada regra é aplicável ou não;
Deve ser possível criar exceções para dispositivos Plug and Play e de armazenamento removível associando o número serial do dispositivo à identidade do usuário, permitindo o uso daquele dispositivo por um usuário específico, mesmo que hajam regras mais gerais de bloqueio;
Deve ser possível bloquear a execução de arquivos a partir de dispositivos removíveis, com a possibilidade de definir exceções à regra.
A identificação de executáveis deve ser dar pelo tipo real do arquivo, independente da sua extensão (filenameextension).
Deve ser possível bloquear o uso de dispositivos de armazenamento removível ou torná-los somente leitura, com a possibilidade de definir exceções baseadas no processo que esteja acessando o dispositivo e também por usuário/número serial do dispositivo;

Inteligência Antimalware e Malha de Comunicação
A solução deve ser capaz de se comunicar com servidor de inteligência antimalware da Rede de Inteligência Antimalware do Estado da Bahiae deve ser integrado com sistema de reputação em nuvem do próprio fabricante;
Atualizações de reputação de arquivos no servidor de inteligência antimalware devem poder ser propagadas em tempo real para todos os sistemas conectados na malha de comunicação;

A malha de comunicação deve ser baseada em protocolo com API/SDK aberta (openDXL) e disponível na Internet, permitindo a integração com outros produtos do mesmo fabricante, produtos de terceiros e desenvolvimento integrações de soluções de segurança pela CONTRATANTE;
A comunicação entre os clientes e os servidores de reputação deve ser bidirecional para permitir consultas ou atualização de informações no servidor de reputação (comunicação 1 para 1) e disseminação de informações do servidor para os clientes (comunicação 1 para N) para informar mudanças de reputação de arquivos e requisições de ações;
Os serviços de reputação devem poder ser integrados, mesmo quando gerenciados por consoles de administração centralizadas distintas;

Funcionalidades de Reconhecimento de Novas Ameaças para Windows Endpoints e Servers
A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações para detecção de malware zero-day;
O cliente deverá possuir módulo de análise que verifique a reputação e imponha regras para execução/bloqueio de arquivos potencialmente maliciosos, com capacidade de conter, bloquear e limpar arquivos baseado na reputação e nos critérios de risco estabelecidos;
Cada vez que um cliente executar um arquivo desconhecido ele deve realizar uma consulta ao servidor de inteligência para obter informações de reputação do arquivo e dos certificados digitais associados;
As ações/políticas a serem executadas a partir da reputação dos arquivos devem poder ser colocadas em modo de observação, de forma que as ações que seriam executadas sejam apenas informadas, de forma a permitir conhecer o ambiente e realizar o ajuste fino da configuração antes da sua aplicação efetiva
A solução deve possuir, pelo menos, 5 níveis de reputação de arquivos;
A depender da reputação do arquivo, deverá ser possível:
Bloquear a execução;
Limpar o arquivo;
Colocar o arquivo em quarentena;
Perguntar ao usuário o que fazer, com possibilidade de envio de mensagem ao administrador;
Permitir a execução;
Permitir a execução em modo controlado (container);
A solução de endpoint avançada deverá possuir módulo de confinamento dinâmico ("container") para execução em modo protegido de arquivos com reputações duvidosas ou desconhecidas, de acordo com as políticas definidas pelo administrador;
A solução deve permitir elevar e rebaixar a reputação de arquivos no servidor de inteligência antimalware, bem como excluir explicitamente um arquivo do processo de confinamento dinâmico, através da console de gerenciamento;
O sistema de confinamento dinâmico deve possuir um conjunto de regras de proteção do sistema e políticas default do fabricante, que podem ser customizadas pelo administrador, com opções de bloquear e somente relatar (report);
Caso as regras de proteção sejam disparadas por uma aplicação, estes eventos deverão contribuir para ajustar a informação de reputação da aplicação;
A solução deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico
A solução deve manter um cache de reputação local - do próprio endpoint - com informações de aplicações - conhecidas, desconhecidas e maliciosas.
Dentre os comportamentos maliciosos, deve ser capaz de realizar, de forma customizada pelo administrador:
Boqueio de acesso local a partir de cookies;
Bloqueio de criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs

Bloqueio de criação de arquivos em qualquer local de rede
Bloqueio de criação de novos CLSIDs, APPIDs e TYPELIBs
Bloqueio de criação de threads em outro processo
Bloqueio de desativação de executáveis críticos do sistema operacional
Bloqueio de leitura/exclusão/gravação de arquivos visados por Ransomwares
Bloqueio de gravação e leitura na memória de outro processo
Bloqueio de modificação da política de firewall do windows
Bloqueio de modificação da pasta de tarefas do Windows
Bloqueio de modificação de arquivos críticos do Windows e Locais do Registro
Bloqueio de modificação de arquivos executáveis portáteis;
Bloqueio de modificação de bit de atributo oculto
Bloqueio de modificação de bit de atributo somente leitura
Bloqueio de modificação de entradas de registro de DLL AppInit;
Bloqueio de modificação de locais do registro de inicialização
Bloqueio de modificação de pastas de dados de usuários;
Bloqueio de modificação do local do Registro de Serviços
Bloqueio de suspensão de um processo
Bloqueio de término de outro processo
Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.
O sistema de detecção avançada deve possuir módulo de detecção de padrões de comportamento malicioso utilizando técnicas de machine-learning;
O sistema de detecção avançada deve ser capaz de coletar e enviar atributos de arquivos e informações de comportamento para o sistema de machine-learning na nuvem do fabricante para análise de malware;
O sistema de detecção avançada deve ser capaz de usar módulo de machine-learning local para detecção de malware;
O modulo de machine-learning deve ser capaz de interagir com os sistemas de reputação local para mitigar falsos positivos;
O sistema de detecção avançada deve ser capaz de operar em contato com a nuvem do fabricante e também de forma somente em contato com os servidores de reputação locais da CONTRATANTE;
Informações de arquivos e certificados devem poder ser enviados para a nuvem do fabricante para otimizar e compor a informação de reputação do servidor de inteligência local;

Console de Gerenciamento
Ser compatível com Microsoft Windows Server 2003 ou superior.
Ser acessível por MMC ou Web (HTTPS).
Ser capaz de instalar remotamente a solução de segurança nas estações e servidores Windows, através de mecanismo próprio, compartilhamento de rede, login script ou GPO de Active directory.
Ser capaz de gerenciar estações de trabalho e servidores (Windows Server) protegidos pela solução antivírus.
Possuir console única de gerenciamento da solução.
Ser capaz de gerar pacotes customizados (autoexecutáveis) contendo as configurações do produto.
Ser capaz de atualizar os pacotes de instalação com as últimas vacinas, para que o pacote utilizado em uma nova instalação já contenha as últimas vacinas lançadas.
Ser capaz de enviar pela rede o agente para instalação/atualização nas máquinas clientes.
Ser capaz de descobrir novas máquinas na estrutura do Active Directory, realizando instalação automatizada do agente nessas máquinas ou via script de logon.
Ser capaz de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção automaticamente ou via script de logon.

Ser capaz de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalhos que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.
Ser capaz de detectar máquinas que ainda não possuam o agente antivírus da solução instalada e possuir mecanismo que possibilite a instalação do agente nessas máquinas.
Ser capaz de agrupar máquinas por características comuns entre si, por exemplo: agrupar máquinas que não possuam o antivírus instalado, agrupar máquinas que não tenham recebido atualizações num período específico de dias, e etc.
Ser capaz de definir políticas de configurações específicas por grupos de estações, permitindo a criação de subgrupos e herança de políticas entre estes grupos e subgrupos.
Ser capaz de informar se o antivírus está instalado nas estações.
Ser capaz de informar se o antivírus está em execução nas estações.
Ser capaz de informar se o antivírus está atualizado nas estações.
Ser capaz de informar o tempo desde a última conexão da máquina com a console de gerenciamento.
Ser capaz de informar o tempo desde a última atualização de vacinas.
Ser capaz de informar o último scan executado na máquina.
Ser capaz de informar a versão do antivírus instalado na máquina.
Ser capaz de informar se é necessário reinicialização para aplicar mudanças provenientes de updates/upgrades.
Ser capaz de informar a quantidade de vírus encontrados na máquina (contador).
Ser capaz de informar o nome do computador.
Ser capaz de informar o domínio ou grupo de trabalho do computador.
Ser capaz de informar versão do sistema operacional.
Ser capaz de informar quantidade de processadores.
Ser capaz de informar quantidade de memória RAM.
Ser capaz de informar instantaneamente os usuários que estão logados, incluindo informações de contato caso disponíveis no Active Directory.
Ser capaz de informar o endereço IP da máquina;
Ser capaz de bloquear as configurações do antivírus instalado de forma que o usuário não consiga alterá-las.
Ser capaz de reconectar as máquinas clientes ao servidor mais próximo.
Ser capaz de configurar políticas que possibilitem que um computador cliente fora da estrutura de proteção possa atualizar-se via internet.
Ser capaz de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.
Ser capaz de relacionar servidores em estrutura hierárquica para obter relatórios sobre toda a estrutura de antivírus.
Ser capaz de herdar tarefas e políticas na estrutura hierárquica de servidores administrativos.
Ser capaz de eleger qualquer computador cliente como repositório de vacinas, sem que seja necessário a instalação de um servidor administrativo completo, onde outras máquinas clientes poderão atualizar-se, para a otimização do tráfego da rede.
Ser capaz de exportar relatórios nos seguintes formatos: HTML e XML.
Ser capaz de enviar e-mails para contas previamente configuradas em caso de alguns eventos.
Ser compatível com Microsoft NAP, quando instalado em servidores Windows 2008.
Ser capaz de detectar anomalias na rede e possuir mecanismo que alerte ao administrador algum evento anômalo.

Cliente para Servidores
Prover compatibilidade para Windows Server 2003 ou superior.
Prover módulo de proteção residente para arquivos que verifique qualquer arquivo criado, acessado ou modificado.

Ser capaz de proteger os processos do antivírus contra ataques.
Prover opções de seleção de módulos a serem instalados nas máquinas clientes durante a instalação, seja está realizada localmente ou remotamente.
As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários, no máximo, a cada hora após a atualização das assinaturas de vírus (independentemente da criticidade da ameaça).
Ser capaz de desabilitar o firewall do Windows para evitar a incompatibilidade com o firewall da solução ofertada.
Ser capaz de bloquear a instalação de outras soluções antivírus para evitar a incompatibilidade e possíveis conflitos com a solução ofertada.
Ser capaz de adicionar pastas a uma área de exceções para evitar que tais locais sejam escaneados, seja por seleção explícita da pasta em questão, ou com base em alguma regra.
Ser capaz de criar lista com os aplicativos considerados confiáveis para a instituição, os quais não terão as atividades de rede, disco e acesso ao registro do Windows monitorados
Ser capaz de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (quedas de energia, erros, etc...).
Ser capaz de desabilitar escaneamento agendado quando estiver sendo alimentado por UPS.
Ser capaz de liberar recursos de hardware para outros aplicativos finalizarem seu processamento caso isso seja requerido durante um escaneamento agendado.
Prover mecanismo de seleção de arquivos a serem escaneados, por exemplo: escanear somente arquivos novos, escanear somente arquivos alterados recentemente, etc...
Ser capaz de escanear objetos usando heurística.
O módulo de proteção de arquivos deverá ao encontrar um objeto perigoso (de acordo com a configuração pré-estabelecida pelo administrador):
Perguntar o que fazer, ou
Bloquear acesso ao objeto, apagar o objeto ou tentar desinfetá-lo.
Caso a desinfecção seja bem sucedida: Restaurar o objeto pra uso.
Caso a desinfecção falhe: Mover para quarentena ou apagar o objeto.
Suporta a realização de um backup do objeto antes de qualquer tentativa de desinfecção ou exclusão permanente.
Suportar IPv6.
Ser capaz de detectar e bloquear arquivos infectados enviados para o servidor.
Prover proteção completa, pronta para operação e contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks).
Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.
Conter no mínimo dois conjuntos de regras de Firewall:
Filtro por pacotes (Portas, protocolos e direção da conexão a ser bloqueada/permitida)
Filtro por aplicação (Controlar o acesso de algumas aplicações específicas a determinadas portas e protocolos)
Ser capaz de detectar e bloquear ações de códigos maliciosos e suas variáveis como, vírus, ransomwares, spywares, rootkits, botnets, backdoors, trojans, worms e etc.

Cliente para Estações de Trabalho e Notebooks
Prover compatibilidade para Windows 7 e versões superiores.
Prover opções de seleção de módulos a serem instalados nas máquinas clientes durante a instalação, seja está feito localmente ou remota.
As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários, no máximo, a cada hora após a atualização das assinaturas de vírus (independentemente da criticidade da ameaça).
Ser capaz de desabilitar o firewall do Windows para evitar a incompatibilidade com o firewall da solução ofertada.

Ser capaz de bloquear a instalação de outras soluções antivírus para evitar a incompatibilidade e possíveis conflitos com a solução ofertada.
Ser capaz de adicionar pastas a uma área de exceções para evitar que tais locais sejam escaneados, seja por seleção explicita da pasta em questão, ou com base em alguma regra.
Ser capaz de criar uma lista com os aplicativos considerados confiáveis para a instituição, os quais não terão as atividades de rede, disco e acesso ao registro do Windows monitorados.
Ser capaz de desabilitar escaneamento agendado quando o notebook estiver funcionando a partir de baterias.
Ser capaz de liberar recursos de hardware para outros aplicativos finalizarem seu processamento caso isso seja requerido durante um escaneamento agendado.
Prover mecanismo de seleção de arquivos a serem escaneados, por exemplo: escanear somente arquivos novos, escanear somente arquivos alterados recentemente.
Ser capaz de escanear objetos usando heurística.
O módulo de proteção de arquivos deverá ao encontrar um objeto perigoso (de acordo com a configuração pré-estabelecida pelo administrador):
Perguntar o que fazer, ou;
Bloquear acesso ao objeto, apagar o objeto ou tentar desinfetá-lo.
Caso a desinfecção seja bem sucedida: Restaurar o objeto pra uso;
Caso a desinfecção falhe: Mover para quarentena ou apagar o objeto;
Antes de qualquer tentativa de desinfecção ou exclusão permanente, a solução deve realizar um backup do objeto.
Possuir mecanismo que identifique páginas web suspeitas, ou que sejam origem de phishing.
Ser capaz de verificar e-mails enviados e recebidos pelos principais protocolos de correio (POP3, SMTP, IMAP).
Ser capaz de verificar o tráfego web nos browsers: Internet Explorer, Firefox e Google Chrome.
Ser capaz de verificar o corpo e os anexos de e-mail usando heurística.
O módulo de email ao encontrar um objeto potencialmente perigoso deve (de acordo com a configuração pré-estabelecida pelo administrador):
Perguntar o que fazer, ou;
Bloquear o email, poderá apagar o objeto ou tentar desinfetá-lo.
Caso a desinfecção seja bem-sucedida: Restaurar o email para o usuário,
Caso a desinfecção não seja possível: Mover para quarentena ou apagar o objeto.
Caso o e-mail contiver código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
Ser capaz de filtrar bloquear anexos de e-mail com a possibilidade de restauração de um anexo filtrado/bloqueado.
Ser capaz de verificar o tráfego HTTP e qualquer script do Windows, usando heurísticas.
Suportar IPv6.
Possuir módulos de monitoramento Web e E-mail.
O módulo de verificação web, ao encontrar código malicioso em alguma página deve (De acordo com as configurações pré-definidas pelo administrador):
Perguntar o que fazer, ou;
Bloquear o acesso ao objeto e mostrar uma mensagem de bloqueio, ou;
Permitir o acesso ao objeto;
Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web.
Ser capaz de monitorar as aplicações instaladas para detectar atividades consideradas perigosas.
Possuir módulos de defesa contra ameaças sem arquivo (Fileless);
Ser capaz de monitorar e bloquear alterações em chaves especificas do registro do Windows.
Prover proteção completa, pronta para operação e contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks).

Ser capaz de analisar os processos e atividades por meio de tecnologias de Machine Learning;
Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.
O módulo Firewall deverá conter no mínimo dois conjuntos de regras:
Filtro por pacotes (Portas, protocolos e direção da conexão a ser bloqueada/permitida)
Filtro por aplicação (Controlar o acesso de algumas aplicações específicas a determinadas portas e protocolos)
Deve possuir módulo que permita restringir o acesso aos seguintes dispositivos externos:
Dispositivos USB;
Drives de CD\DVD-ROM;
Drives de disquete;
Dispositivos IEEE 1394(Firewire);
Modems;
Dispositivos COM e LPT;
Leitores de cartão (SD, MemoryStick, etc)
Dispositivos Bluetooth.
Ser capaz de detectar e bloquear ações de códigos maliciosos e suas variáveis como, vírus, ransomwares, spywares, rootkits, bootnets, backdoors, trojans, worms e etc.
Possuir módulo de prevenção ao vazamento de dados (DLP);
Ser possível de rodar arquivos desconhecidos em ambiente virtualizado (container) impedindo o mesmo de interagir fora da virtualização;
Possuir a capacidade de emular sandbox local e em nuvem;

(04) Prazo, local e condições de entrega ou execução: Dez dias após assinatura do contrato., na Prefeitura Municipal de Xanxerê – Departamento de Informática.

(05) Condições de garantia

O licitante deverá prestar assistência técnica por telefone e acesso remoto, quando necessário, durante o período de vigência contrato, sendo que os prazos serão contados a partir da data de emissão do Termo de Recebimento Definitivo de Bens. Não obstante, também com relação ao cumprimento da garantia, a(s) empresa(s) contratada(s) fica(m) sujeita(s) às disposições contidas no respectivo Contrato.
A CONTRATADA deverá arcar com todos os custos e despesas inerentes à prestação do serviço de garantia acima citado, tais como deslocamentos, alimentação, hospedagem, fretes, etc.
Durante o período de vigência contratual, o fornecedor ficará obrigado a efetuar, às suas expensas, a substituição ou reparo de todo e qualquer componente que apresente defeito de fabricação, bem como possíveis correções no software para o perfeito funcionamento da solução, regularmente constatado.
Além da obrigação de prestação de garantia, a CONTRATADA também se obriga a respeitar o prazo MÁXIMO DE 2 (duas) HORAS, contadas da data de cada chamado, para atendimento remoto ou telefônico.
A CONTRATADA deverá solucionar o problema que resultou no chamado técnico, no prazo máximo de 02 (DOIS) DIAS ÚTEIS, contados a partir da data de comparecimento, registrada pelo servidor que fez o chamado.
Na hipótese de subcontratar a assistência técnica para a prestação do serviço, a CONTRATADA deverá entregar à CONTRATANTE cópia autenticada ou via original do pertinente instrumento particular de contrato firmado entre ela (CONTRATADA) e a empresa terceirizada (com firmas devidamente reconhecidas em cartório), sob pena de rescisão unilateral do presente Termo Contratual, sem prejuízo das sanções dispostas nos artigos 86 e 87 da Lei Federal nº 8.666/93.

PREFEITURA DE
XANXERÊ

A CONTRATADA deverá fornecer relatórios de serviços executados, assumir todos os possíveis danos, tanto nas dependências físicas, quanto bens materiais, causados a CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança quando da execução dos serviços;

(06) Responsável pelo recebimento, telefone e e-mail – **Gestor e Fiscal do Contrato**

Anderson Orso – CPF: 043.012.649-22- Telefone: 3441-8500

(07) Condições e prazos de pagamento:

Conforme Decreto n° 072/2021

(08) Dotação Orçamentária Rud 13 d.00 3390317

(09) Obrigações da contratante

Efetuar pagamento conforme cronograma;
Fiscalizar a execução do objeto;

(10) Obrigações da contratada

Prestar os serviços de forma continua;
Realizar suporte técnico quando necessário;

(11) Qualificação técnica:
Credenciamento no fabricante.

(12) Critério de avaliação das propostas

Menor preço.

(13) Valores referenciais de mercado

Secure Gate – Cyber Security – CNPJ: 24.832.664/0001-85 – Valor: 15.250,20.
Consultoria Verum – CNPJ: 27.617.022/0001-51 – Valor 15.890,00

(14) Estimativa de Custo
Menor preço: R$ 15.250,20

(15) Prazo de Vigência do Contrato: 36 meses.

(16) Resultados esperados:

Fornecer segurança cibernética nos dados da prefeitura;

PREFEITURA DE
XANXERÊ

Proteger a integridade dos arquivos e comunicações internas;
Suporte técnico

(17) Responsável por informações sobre o objeto: Anderson Orso – 3441-8500 – 7:00 às 13:00.

Data: 22/02/2021

Adenilso Biasus
Assinatura do Secretário

Ciente:
Oscar Martarello
Prefeito Municipal

Anderson Orso
Assinatura do Fiscal

CONSULTORIA V

CONSULTORIA VERUM
Rua Tadeu Milan, 104
(41) 99623-9239

PROPOSTA COMERCIAL

29/01/2021

PARA: Prefeitura Municipal de Xanxerê
A/C: Anderson Orso – Departamento de Informática

Serviço/Produto	Quantidade	Valor Unitário	Valor Unitário
Comodo Advanced Endpoint Protection - Premium Edition para 36 meses.	140	R$ 113,50	R$ 15.890,00
		TOTAL	15.890,00

Período de Licenciamento: 36 meses.
Validade da Proposta: 10 dias.
Condição de Pagamento: 30 dias.
Taxas/Impostos: Incluso
Suporte Técnico: Incluso serviço remoto 8x5.

Nos colocamos, desde já a disposição para quaisquer esclarecimentos que se façam necessários.

Cordialmene,
Consultoria Verum

De acordo em: ___/___/_____

_____
Pref. Munic. De Xanxerê

CONSULTORIA V

Proposta Comercial

securegate
cyber security

Número da Proposta:	Responsável:	Data:	Data de Expiração:
SG-013/2021- XANXERE (COMODO)	Caroline Prado carol@securegate.com.br	28-jan-2021	04-fev-2021

Preparado para:
XANXERE
informatica@xanxere.sc.gov.br
A/C Anderson Orso

Product Description	Start Date	End Date	Net Price Unit	Quantity	Term (months)	Line Total
Comodo Advanced Endpoint Protection - Premium Edition	28-Jan-2021	27-Jan-2024	R$ 108,93	140	36 meses	R$ 15.250,20
					TOTAL	**R$ 15.250,20**

Validade da Proposta: 7 dias
Condição de Pagamento: 28 dias.
Dados para faturamento: Secure Gate
R. Ubaldino do Amaral, 927, sala 20
CEP 80045-070 - Alto da Rua XV -
Curitiba - PR
CNPJ 24.832.664/0001-85

Taxas/Impostos: incluso de todos os impostos, taxas, encargos e demais despesas.
Suporte Técnico: atendimento remoto através de e-mail e telefone, na modalidade 8x5.

Quaisquer informações sobre as especificações técnicas e preços ofertados deverão ser dirigidas no telefone (41) 3148-6950 ou no e-mail: comercial@securegate.com.br.

Atenciosamente,

Carol Prado

carol@securegate.com.br

Secure Gate Cyber Security
Rua Fernando Amaro, 60
Curitiba-PR

securegate
cyber security

PREFEITURA DE
XANXERÊ

TERMO DE REFERÊNCIA

Unidade Requisitante: Secretaria de Administração e Finanças

Ordenador da despesa: Adenilso Biasus

(01) Objeto: Aquisição de licenciamento da Veeam Backup Essentials Standard 2 socket bundle para VMware e do licenciamento da VMware vSphare 6 Essentials kit.

(02) Motivação/Justificativa

A pretendida contratação faz-se indispensável, pois visa prover segurança, proteção dos dados produzidos e armazenados no servidor do município de Xanxerê, além disso, tanto o Veeam Backup como o hypervisor são soluções utilizadas pelo município há mais de 3 anos, e assim fica inviável substituir a mesma.

(03) Especificações técnicas:

Renovação de licenciamento da Veeam Backup Essentials Standard 2 Socket Bundler para VMware

Manutenção de segurança de dados do ambiente virtualizado para criação de ambiente de cópia / recuperação (backup/restore), local e remoto, para discos e unidade de fitas e solução de replicação/DR (Disaster Recovery) entre estruturas heterogêneas;
Atualização e suporte para software de backup de maquinas virtuais e replicação;
Garantia e suporte e atualização de 3 anos para o software com as mesmas características;
Tempo de resposta dos chamados de 2 horas;
Disponibilidade de suporte 12 horas por dia de segunda a sexta;

Renovação de licenciamento da VMware vSphere 6 Essentials Kit

Software de gerenciamento de rede para criação de máquinas virtuais com até dois processadores em todos os sistemas operacionais suportados;
Fornecimento de correções, novas versões, releases ou atualizações mais recentes comercialmente disponíveis dos produtos durante o período de vigência dos serviços;
Suporte técnico básico 24 horas por dia, 7 dias por semana (24 x 7), para resolução de problemas.
Garantia e suporte e atualização de 3 anos para o software com as mesmas características;

(04) Prazo, local e condições de entrega ou execução: Dez dias após assinatura do contrato., na Prefeitura Municipal de Xanxerê – Departamento de Informática.

(05) Condições de garantia

O licitante deverá prestar assistência técnica por telefone e acesso remoto, quando necessário, durante o período de vigência contrato, sendo que os prazos serão contados a partir da data de emissão do Termo de Recebimento Definitivo de Bens. Não obstante, também com relação ao

cumprimento da garantia, a(s) empresa(s) contratada(s) fica(m) sujeita(s) às disposições contidas no respectivo Contrato.
A CONTRATADA deverá arcar com todos os custos e despesas inerentes à prestação do serviço de garantia acima citado, tais como deslocamentos, alimentação, hospedagem, fretes, etc.
Durante o período de vigência contratual, o fornecedor ficará obrigado a efetuar, às suas expensas, a substituição ou reparo de todo e qualquer componente que apresente defeito de fabricação, bem como possíveis correções no software para o perfeito funcionamento da solução, regularmente constatado.
Além da obrigação de prestação de garantia, a CONTRATADA também se obriga a respeitar o prazo MÁXIMO DE 2 (duas) HORAS, contadas da data de cada chamado, para atendimento remoto ou telefônico.
A CONTRATADA deverá solucionar o problema que resultou no chamado técnico, no prazo máximo de 02 (DOIS) DIAS ÚTEIS, contados a partir da data de comparecimento, registrada pelo servidor que fez o chamado.
Na hipótese de subcontratar a assistência técnica para a prestação do serviço, a CONTRATADA deverá entregar à CONTRATANTE cópia autenticada ou via original do pertinente instrumento particular de contrato firmado entre ela (CONTRATADA) e a empresa terceirizada (com firmas devidamente reconhecidas em cartório), sob pena de rescisão unilateral do presente Termo Contratual, sem prejuízo das sanções dispostas nos artigos 86 e 87 da Lei Federal nº 8.666/93.
A CONTRATADA deverá fornecer relatórios de serviços executados, assumir todos os possíveis danos, tanto nas dependências físicas, quanto bens materiais, causados a CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança quando da execução dos serviços;

(06) Responsável pelo recebimento, telefone e e-mail – **Gestor e Fiscal do Contrato**

Anderson Orso – CPF: 043.012.649-22- Telefone: 3441-8500

(07) Condições e prazos de pagamento:

Conforme Decreto nº 072/2021

(08) Dotação Orçamentária rect. 13 d.00 33903017

(09) Obrigações da contratante

Efetuar pagamento conforme cronograma;
Fiscalizar a execução do objeto;

(10) Obrigações da contratada

Prestar os serviços de forma continua;
Realizar suporte técnico quando necessário;

(11) Qualificação técnica:

Credenciamento no Fabricante.

PREFEITURA DE
XANXERÊ

(12) Critério de avaliação das propostas

Menor preço.

(13) Valores referenciais de mercado

CBA Informática – CNPJ: 80.156.326/0001-41 – Valor: 11.150,00.

Foi solicitado para outras empresas efetuarem cotação e até o momento nenhuma retornou os e-mails, conforme documentação em anexo.

(14) Estimativa de Custo

R$ 11.150,00 (onze mil cento e cinquenta reais)

(15) Prazo de Vigência do Contrato: 36 meses.

(16) Resultados esperados:

Fornecer segurança cibernética nos dados da prefeitura;
Proteger a integridade dos arquivos e comunicações internas;
Suporte técnico

(17) Responsável por informações sobre o objeto: Anderson Orso – 3441-8500 – 7:00 às 13:00.

Data: 25/02/2021

Adenilso Biasus
Assinatura do Secretário

Ciente:
Oscar Martarello
Prefeito Municipal

Anderson Orso
Assinatura do Fiscal

CBA INFORMÁTICA LTDA
Rua Oslo 90 D - Passo dos Fortes
Chapecó – SC - Fone: (49) 3321.4774
CNPJ: 80.156.326/0001-41 – I.E 251.591.336

PROPOSTA/PEDIDO Nº P0007 C

NOME:	PREFEITURA MUNICIPAL DE XANXERÊ					DATA:	25/01/2021
CPF/CNPJ:	83.009.860/0001-13	I.E:	ISENTA			CÓDIGO:	
END. RUA:	RUA JOSÉ DE MIRANDA RAMOS					Nº:	455
BAIRRO:	CENTRO		CIDADE:	XANXERÊ			
COMPLEMENTO:			CEP:	89.820-000		UF:	SC
FONE FIXO:	(49) 3441 8516		FONE CEL:			CONTATO:	ANDERSON
EMAIL/OBS.:	ti@xanxere.sc.gov.br						

QTD	DESCRIÇÃO DO PRODUTO	UNITARIO	TOTAL
02	Renovação de licenciamento da Veeam Backup Essentials Standard 2 socket bundle para VMware • Manutenção de segurança de dados do ambiente virtualizado para criação de ambiente de cópia / recuperação (backup/restore), local e remoto, para discos e unidade de fitas e solução de replicação/DR (Disaster Recovery) entre estruturas heterogêneas de diferentes fabricantes. • Atualizações e suporte básico para o Software de Backup de Máquinas Virtuais e Replicação; • Garantia e suporte adicional de 2 anos para o software com as mesmas características, totalizando 3 anos de garantia e suporte. • Tempo de resposta: 2 horas • Disponibilidade: 12 horas por dia (8h00 - 20h00) / segunda a sexta-feira. • Quantidade de licença: 2 soquetes	4.880,00	9.760,00
01	Renovação de licenciamento da VMware vSphere 6 Essentials Kit • Software de gerenciamento de rede para a criação de máquinas virtuais com até 2 (dois) processadores em todos os sistemas operacionais suportados. • Fornecimento de correções, novas versões, releases ou atualizações mais recentes comercialmente disponíveis dos produtos durante o período de vigência dos serviços; • Suporte técnico básico 24 horas por dia, 7 dias por semana (24x7), para resolução de problemas por um período de 3 anos de suporte.	1.390,00	1.390,00

VALOR DA PROPOSTA: R$ 11.150,00 (Onze mil e cento e cinquenta Reais)

Prazo de Entrega: 29/01/2021
Forma de Pagamento: 20/02/2021
Frete: CIF - (Pago).
Validade da Proposta: 10 dias corridos.

80.156.326/0001-41
CBA INFORMÁTICA LTDA.
R: Oslo, 90-D
B: Passo dos Fortes - CEP 89.805-110
CHAPECÓ - SC

Atenciosamente,