Zimbra **luynne.cardoso@sead.pi.gov.br**

Impugnação - EDITAL DE LICITAÇÃO Nº 34/2023/SEAD PROCESSO Nº 00309.003071/2023-02

De : VIXBOT <licita@vixbot.com.br> sex., 22 de dez. de 2023 11:36

Assunto : Impugnação - EDITAL DE LICITAÇÃO Nº 34/2023/SEAD PROCESSO Nº 00309.003071/2023-02 4 anexos

Para : luynne cardoso <luynne.cardoso@sead.pi.gov.br>

Srta Pregoeira,

Cumprimentando-a, cordialmente, vimos tempestiva e mui respeitosamente, apresentar pedido de impugnação ao presente certame.

Cordiais agradecimentos,

Departamento Governo
E-mail: licita@vixbot.com.br
Tel (+55) 61 – 3968.9990
www.vixbot.com.br

Imprima com responsabilidade, preserve o meio ambiente !!!

Impugnação - SEAD Piaui.pdf
371 KB

Catalogo BluePex.pdf
399 KB

ILUSTRÍSSIMO SENHOR PREGOEIRO DA SECRETARIA DE ADMINISTRAÇÃO DO ESTADO DO PIAUÍ

EDITAL DE LICITAÇÃO Nº 34/2023/SEAD
PROCESSO Nº 00309.003071/2023-02

A **VIXBOT SOLUÇÕES EM INFORMÁTICA LTDA**, inscrita no CNPJ sob n° 21.997.155/0001-14, por intermédio de seu (a) representante legal o (a) Senhor (a) Marina Nova da Costa Mendes, portador (a) da Carteira de Identidade n° 2117819 – SSPDF e do CPF n° 007.399.241-09, vem tempestiva e mui respeitosamente à presença de Vossa Senhoria, apresentar **IMPUGNAÇÃO AO EDITAL** com fulcro no Edital, bem como demais legislações pertinentes à matéria.

I– DOS FATOS:

Inicialmente, pertinente ressaltar que esta Signatária, atua no varejo eletrônico há mais de 8 (oito) anos, contemplando o fortalecimento das relações com o mercado governamental e corporativo, primando pela excelência dos trabalhos prestados. Diante disso, em razão de sua expertise no atendimento aos Órgão Públicos, tem interesse em participar do Pregão Eletrônico nº 34/2023 cujo objeto é promover "a escolha da proposta mais vantajosa para a aquisição do objeto descrito na Parte Específica deste Edital, conforme condições, quantidades e exigências estabelecidas no Anexo I – Termo de Referência"

Todavia, observou-se que o presente Edital apresenta algumas inconstâncias e, para que não ocorra a preclusão do direito, impugna-se o presente Edital, conforme passa a expor

II - DO DIREITO:

Conforme previsão da legislação em vigor e do instrumento convocatório descrito no capítulo 10. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO:

> **10.1. Qualquer pessoa poderá impugnar os termos deste Edital, por meio eletrônico, até 03 (três) dias úteis antes da data designada para a abertura da sessão pública.**

Tem-se, portanto, que o presente pleito congloba todos os parâmetros elencados nas disposições normativas supra, visto tratar-se de impugnação por meio do qual se opõe a atos administrativos irregulares praticados por autoridade da **SECRETARIA DE ADMINISTRAÇÃO DO ESTADO DO PIAUÍ**, que cerceiam a livre participação de licitantes no âmbito de certame licitatório na modalidade Pregão Eletrônico, e ensejam uma miríade de prejuízos financeiros de incalculável monta, em decorrência do mau emprego dos

recursos do Erário, sendo, portanto, todas as nuances da presente lide atinentes ao Direito Público.

A IMPUGNANTE busca resguardar seus direitos, enquanto licitante, à escorreita observância de todas as disposições normativas da Lei nº 8.666/93, da Lei nº 10.520/02, do Decreto Federal nº 10.024/19 e das disposições do Edital, nos atos administrativos procedimentais devidos e pertinentes no âmbito do certame licitatório em comento, em prestígio aos princípios jurídicos administrativos da isonomia, da legalidade, da impessoalidade, da moralidade e da probidade, da publicidade, do julgamento objetivo, da livre concorrência, da vinculação ao instrumento licitatório, da ampla defesa e do contraditório, da economicidade e da escolha da proposta mais vantajosa.

Nos moldes do que restará comprovado pelas razões de direito a seguir delineadas, a impugnante postula a imediata reforma da decisão que obliterou seu direito à observância às disposições legais e editalícias pertinentes à fase recursal do Pregão Eletrônico em comento.

Nessa toada, a impugnante aduz, desde já, que, data maxima venia, as condutas do Pregoeiro e das demais autoridades administrativas que atuam na condução do Pregão que perpetram feridas mortais a toda sorte de dispositivo normativo pertinente, mormente os princípios da ampla participação, da economicidade, do julgamento objetivo, bem como às contas da SECRETARIA DE ADMINISTRAÇÃO DO ESTADO DO PIAUÍ.

Em assim sendo, busca a impugnante a tutela dos incontestáveis direitos subjetivos enquanto licitante, em face de ato cerceador de autoridades públicas, ao periélio das disposições do instrumento convocatório regente do certame, bem como das disposições normativas da Lei nº 8.666/93, da Lei nº 10.520/02, as disposições principiológicas administrativas pertinentes e, ad corolarium, as disposições do artigo 37 da Constituição Federal de 1988.

III - DAS RAZÕES PARA A PRESENTE IMPUGNAÇÃO:

Em verificação às exigências constantes no edital, notou-se que há limitação do número de participantes, pois às especificações constantes para a solução de software pretendida **só podem ser atendidas pela fabricante BluePex por meio da aplicação End Point Control & Protection**, deixando de fora da competição outras fabricantes do ramo, violando assim a isonomia e competitividade.

Se as especificações são extremamente necessárias, deve-se apresentar a análise de viabilidade técnica e econômica que o Órgão deve proceder, em conformidade com a Instrução Normativa n° 04, de 12 de novembro de 2010.

Além do direcionamento da solução de software, ainda, o edital de licitação traz exigências que já foram amplamente debatidas pela Corte de Contas, as quais, reconhecidamente, ferem os princípios que devem por reger os processos de compras públicas.

Traremos à tona, certas atrocidades contidas no instrumento convocatório, tidas como restritivas à competitividade e a legalidade do certame em tese, senão vejamos:

> ***Anexo - TERMO DE REFERÊNCIA***
>
> ***Itens 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124:***
>
> ***12. Softwares Inclusos:***
> ***12.2. Acompanha Software de segurança e Monitoramento, conforme Anexo I A.***
>
> ***Anexo I A***
>
> ***Considerar toda a descrição da solução constante em 6 páginas do Anexo I A.***

Conforme documento anexado a presente impugnação, o software descrito no Anexo I A fora flagrantemente copiado da solução da **fabricante BluePex por meio da aplicação End Point Control & Protection**. Além do direcionamento a uma única solução, ainda, foram implantadas exigências que limitam a participação de diversas empresas e, por que não dizer, que restringe o pleno cumprimento a uma única empresa a ser escolhida por este fabricante:

> ***1.3. Apresentar Carta emitida pelo próprio Fabricante, dirigida ao LICITANTE, referenciando ao edital em epígrafe, informando que a Proponente é revenda autorizada a comercializar seus produtos e serviços, e o Fabricante confirma que atende a todos os itens listados no referente edital. Tal documento deverá ser anexado aos documentos de habilitação.***
>
> ***1.4. Será feita a verificação da compatibilidade dos recursos e das capacidades, facilidades operacionais informadas na proposta para cada item ofertado com base nas informações dos catálogos, folhetos, manuais técnicos e semelhantes produzidos pelo fabricante. Apresentar no mínimo 1 técnico certificado em todas as soluções ofertadas. Este deverá ser comprovado através de documento emitido pelo fabricante da solução ou empresa devidamente autorizada para emissão de certificados.***

Ao que se refere ao direcionamento do software a uma única solução existente no mercado, o Tribunal de Contas da União no Acórdão 2829/2015 se debruçando sobre o tema, decidiu:

> **"**No planejamento de suas aquisições de equipamentos, a Administração deve identificar um conjunto representativo dos diversos modelos existentes no mercado que atendam completamente suas necessidades antes de elaborar as especificações técnicas e a cotação de preços, de modo a caracterizar a realização de ampla pesquisa de mercado **e evitar o direcionamento do certame para modelo específico** pela inserção no edital de características atípicas."(***Acórdão 2829/2015-Plenário, TC 019.804/2014-8, relator Ministro Bruno Dantas, 04.11.2015.)***

Tendo em vista a inexistência de algum outro produto que atenda todas as exigências do Edital, torna-se, consequentemente, impossível que seja respeitado o princípio constitucional da ampla concorrência e competitividade real, perdendo assim a finalidade da licitação.

Outra pauta alvo de ataque no presente documento é a necessidade de apresentação de carta emitida pelo fabricante dirigida ao LICITANTE, referenciando ao edital em epígrafe, informando que a Proponente é revenda autorizada a comercializar seus produtos e serviços. Esta pauta já foi amplamente debatida e rechaçada pela Corte de Contas, onde entre a coleção de pareceres sobre o tema, escolhemos enfatizar o que possivelmente mais se aplica ao processo em tese, através do Acórdão nº. 423/2007, in verbis:

> **"A declaração (do fabricante) confere poder demasiado e irrestrito ao fabricante dos equipamentos, o qual poderia, por questões mercadológicas, comerciais ou outras quaisquer, simplesmente deixar de "habilitar" algumas empresas tecnicamente aptas para a prestação dos serviços ou, ainda, escolher determinados "parceiros" que considere mais adequados para representá-la e comercializar seus produtos e serviços, em detrimento de outras empresas com iguais capacidades técnicas. (...) abstenha-se de exigir, portanto, no ato convocatório, que as empresas licitantes e/ou contratadas apresentem declaração, emitida pelo fabricante do bem ou serviço licitado, de que possuem plenas condições técnicas para executar os serviços, são representantes legais e estão autorizadas a comercializar ou produtos e serviços objeto do termo de referência, uma vez que essa exigência restringe o caráter competitivo do certame."**

Ou seja, manter o edital da forma como fora inicialmente redigido, é corroborar a criação de um cenário em que transfere o poder de decisão ao fabricante da solução quanto a escolha do parceiro de negócio mais conveniente a representá-lo na licitação, refutando a participação de outras licitantes que poderiam ofertar um preço mais vantajoso, mas que terão sua participação cerceada por não obter o documento exigido para habilitá-lo no processo.

Até mesmo porque a Lei 8.666/1993 contém um rol taxativo de documentos de habilitação que podem ser exigidos dos licitantes e imputar documentos não previstos tem por ferir a legalidade do processo licitatório. Pauta esta, inclusive, que também já foi amplamente

debatida pela Corte de Contas, onde está mais do que clara a condição de que é vedado aos agentes públicos admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo.

Face as considerações noticiadas em supra, passamos agora a indagar o critério de julgamento ao se incluir num mesmo item soluções de hardware e software, o que propicia a interrupção de um julgamento objetivo e tende a onerar as ofertas dos licitantes. Ora, ao descrever os mencionados itens 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, com especificações técnicas que contemplam tanto hardware quanto software, descaracterizam totalmente o objeto da licitação.

Em analise as características técnicas solicitadas no hardware e suas certificações, fica claro de que se trata de equipamentos de 1ª linha, de fabricantes notoriamente capazes de fornecer na qualidade exigida. Entre eles citamos, HP, DELL, LENOVO. Contudo, quando se descreve dentro das especificações dos equipamentos os serviços de software, descaracteriza o objeto pretendido, vez que estes serviços não serem contemplados por nenhum deles de maneira original de fábrica.

Para o melhor aproveitamento dos recursos públicos e correto andamento do certame, é necessário que ele seja revisto e republicado de modo que estes serviços sejam licitados em lote/item separado, pois como enfatizado, os fabricantes dos hardwares e suas revendas autorizadas não comercializam os serviços com os desktops. Por outro lado, empresas especialistas nos serviços de tecnologia da informação não comercializam os hardwares.

Para ilustrar o severo equívoco na construção do Termo de Referência, suponhamos que o processo não esteja direcionado a um único fabricante de software e que outras empresas possam ofertar soluções distintas que atentam plenamente os requisitos exigidos. Suponhamos, ainda, que 26 (vinte e seis) fornecedores distintos sejam os detentores dos itens alvo deste debate em que, por sua vez, sejam 26 (vinte e seis) soluções de software diferentes. Questiona-se: Como vosso órgão conseguirá trabalhar com todos esses tipos de software de segurança e gerenciamento ao mesmo tempo? Como se dará o treinamento para 26 (vinte e seis) soluções de software diferentes? Como gerenciar 26 (vinte e seis) soluções de software diferentes para 26 (vinte e seis) soluções de hardware diferentes?

Essa situação acaba impossibilitando a interpretação objetiva do edital, de forma a apresentar a melhor solução que poderia atendê-lo, prejudicando a formulação de propostas nos exatos termos do instrumento convocatório.

Sendo assim, postula-se pela REGULARIZAÇÃO DO EDITAL, sendo retificadas as especificações restritivas da competição, referente ao objeto requerido.

III – DOS PEDIDOS

Ante o acima exposto, vem à presença de Vossa Senhoria, com o devido respeito e acatamento, certos pela adoção de conduta responsável quanto ao seu julgamento, em período em que o Tribunal de Contas do Estado do Piauí encontra-se em recesso de final

de ano e impedido de ser noticiado dos fatos supracitados, onde pedimos conhecer a Impugnação e julgá-la PROCEDENTE.

a) Sejam retificadas as especificações técnicas contidas para os itens 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, conforme as recomendações da impugnante, eis que nenhuma outra marca, além da fabricante BluePex, atende ao exigido em Edital;

a.1) Caso não seja este o entendimento, faz-se necessário que esta Administração indique ao menos três modelos com as respectivas marcas que atendam ao presente Edital;

b) Sejam categorizados em itens distintos as soluções de hardware e de softwares pretendidos nesta contratação;

c) Seja respeitado o prazo para resposta desta impugnação, conforme estabelece a lei; e

d) De qualquer decisão proferida sejam fornecidas as fundamentações jurídicas da resposta e todos os pareceres jurídicos a este respeito.

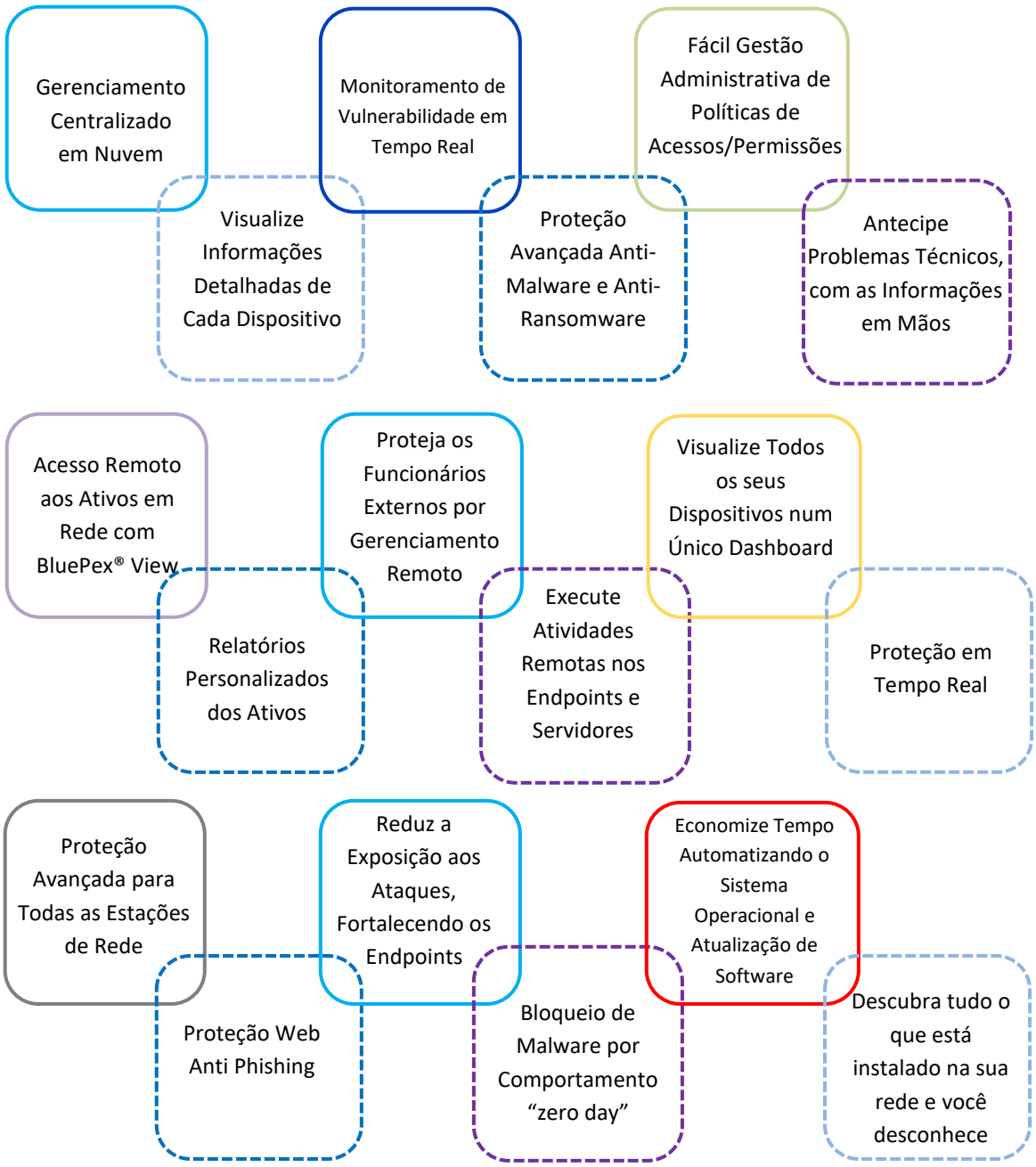
Nestes termos, requer deferimento.

Brasília, 22 de dezembro de 2023

MARINA NOVA DA COSTA MENDES
DIRETORA

BluePex® Endpoint Protection & Control: A plataforma mais completa em proteção e gerenciamento centralizado em nuvem

Oferecemos uma proteção robusta para todo o seu ambiente de TI, o melhor gerenciamento centralizado de endpoints e servidores em nuvem. Protegemos todos os níveis da sua rede. Garantimos que os usuários estejam protegidos e livres de ameaças, em qualquer lugar.



Proteção de quatro camadas em tempo real

+300.000 ameaças novas diariamente

1ª proteção

Proteção de navegação

Bloqueio a sites perigosos e acessos fraudulentos para evitar phishing e downloads por acidente de malwares ou qualquer outro tipo de software malicioso, o BluePex® Endpoint Protection impedirá que se conecte e seja infectado.

2ª proteção

Arquivos vigiados

Os scaners verificam e testam tudo o que foi baixado, usando dois mecanismos de detecção com mais de 10 milhões de padrões, verifica todos os arquivos baixados.

3ª proteção

Bloqueio de comportamento & Verificação em nuvem

Prevenção contra novos malwares e ataques sofisticados através de vulnerabilidades como o dia zero. O dia zero é vulnerabilidade desconhecida, que é usada como inteligência artificial heurística, bloqueio pelo comportamento duvidoso, emitindo um alerta de suspeita.

4ª proteção

Anti-Ransomware

O monitoramento comportamental personalizado impede o Ransomware antes de sequestrar seus dados.

Gerenciamento Centralizado

Dashboard Unificado	Layout clean, simples, intuitivo e gráfico de fácil leitura, mostrando ao profissional de TI a atual condição da segurança de sua infraestrutura.
Controle Granular	Permite controle granular e definição de políticas em vários níveis hierárquicos.
Gerenciamento de Políticas	Permite gerenciar políticas de real time, lista brancas, lista negras, entre outras funções

Detectando e Removendo Malware

Varredura de Vírus e Malwares	Mecanismo de varredura de alta tecnologia que detectam todos os tipos de softwares maliciosos como vírus, trojans, bots, ransomware, spyware, keyloggers e etc.
Escaneamento Rápido	Diferente de outras soluções do mercado, o BluePex® Endpoint Protection, trabalha com um eficiente mecanismo que varre até o nível mais baixo, evitando assinaturas de detecção duplicadas e otimizando a memória.
Detecção de Rootkit	Escaneia setores de inicialização em busca de rootkits que se ocultam no funcionamento do sistema. A leitura é realizada direto no disco rígido
Detecção de PUPs	Alerta o usuário sobre programas potencialmente indesejados (PUPs), por exemplo as barras de ferramentas que se instalam no navegador, adwares e sistemas manipuladores que sobrecarregam a máquina.
Limpeza Avançada de Infecção	Rotinas inteligentes que garantem uma limpeza segura, sem arriscar a estabilidade do computador. São mais de 70 pontos de carregamento (autorun). Restaura valores padrões caso seja necessário.

Prevenindo Novos Malware

Proteção Contra Malware em Tempo Real	Sistema de quatro camadas incluindo proteção de navegação de arquivo e bloqueio de comportamento. As camadas se complementam para uma melhor performance.
Camada 1: Proteção de Navegação	Bloqueio de acesso a sites fraudulentos conhecidos e perigosos evitam fraudes como roubo de senha (phishing) e disseminação perigosa de malwares.
Camada 2: Proteção de Arquivos	Digitaliza todos os arquivos baixados e iniciados usando milhões de assinaturas de malwares. Modos de scan: 1. Apenas quando o programa for iniciado; 2. Verifica todos os arquivos recém-criados e modificados; 3. Verifica todos arquivos enquanto são lidos.
Camada 3: Bloqueio por Comportamento	Localiza novos malwares monitorando o comportamento de todos os programas em execução. Utilizando a base de dados disponível em nuvem para verificação em tempo real
Camada 4: Anti-Ransomware	Bloqueia trojans que tentam fraudar suas transações bancárias. Característica específica do bloqueio de comportamento que detecta manipulações de processo do navegador.
Proteção de Internet Banking	Bloqueia trojans que tentam fraudar suas transações bancárias. Característica específica do bloqueio de comportamento que detecta manipulações de processo do navegador.
Proteção de phishing e Keylogger	Evita roubo de senhas de suas contas online. Característica combinada das três camadas.
Prevenção Contra Manipulação de Exploração e Sistema	Garante a integridade dos dados e a validade dos programas ativos. Detecção combinada de injetores de códigos, exe-patchers, rootkits ocultos, autoruns, switches de hots, trocadores de configurações do navegador e de políticas de grupo e instaladores invisíveis.
Atualizações Automáticas	Proteção contra as mais de 300 mil novas ameaças e sites perigosos que são criados todos os dias. As assinaturas de detecção são atualizadas diariamente.

Vantagens

Análise Programada	Examine a máquina por complete toda sexta-feira à noite após o trabalho, por exemplo. Opção de agendamento de varredura total do sistema.
Configurações para Usuários Avançados	As configurações de fábrica atendem a maioria dos usuários, contudo os usuários avançados podem personalizar as opções de proteção padrão.
Quarentena	Também permite que você envie arquivos para uma análise manual pela BluePex®. Os objetos detectados são mantidos em arquivo seguro criptografado para que uma pesquisa mais aprofundada aponte se deverão ser removidos.
Log Avançado	Útil para o suporte reproduzir o cenário. Mantém registros de todas as atividades de proteção em tempo real, varreduras, quarentena e atualizações.
Notificações	Grande vantagem em relação ao Windows Defender, que não notifica nada. Informa quando um site perigoso for bloqueado ou quando um arquivo baixado foi automaticamente colocado em quarentena.
Permissões	Inclui suporte para usuários e grupos do Active Directory; essencial para as empresas. Defina uma senha de administrador ou restrinja usuários individuais de acessar recursos específicos do software.
Interface Amigável	Uma interface de usuário clean, moderna, simples e fácil de mexer. O BluePex® Endpoint Protection protege qualquer nível de usuário com suas configurações de fábrica, não precisa ser um expert.
100% de Performance	O BluePex® Endpoint Protection foi projetado para usar baixos recursos de sua máquina. Este ganho em eficiência possibilita maior velocidade e um aumento nas taxas de detecção.
Gerenciamento Centralizado em Nuvem	Gerencie a segurança dos endpoints, dispositivos móveis e servidores de arquivos remotamente, em tempo real, de onde estiver, com o BluePex® Cloud Suite.
Varredura de Linha de Comando	A varredura da linha de comando do BluePex® Endpoint Protection possui ótimo desempenho, é conhecida por ser uma das interfaces mais sofisticadas e flexíveis do mercado.

Benefícios para o Usuário

Garantia de tecnologia	Você recebe novas versões de software sem custo dentro do licenciado período, usando apenas o recurso de atualização integrado. A BluePex® não vende apenas software - mas é comprometida pela sua segurança
Suporte Fenomenal ilimitado	Sem limites de chamados, sem robotização no atendimento. A BluePex® Suporte Fenomenal, o suporte é humanizado, com profissionais de TI prontos para te ajudar, você escolhe como será atendido, por: chat, telefone, e-mail. Atendimento remoto ou presencial, no formato 8x5 ou 24x7. Enquanto a correção estiver em andamento, é possível, solicitar uma máquina reserva. Sua empresa nunca para.

Requisitos de Sistema

OS: Windows 7, 8, 8.1, 10
HDD: ~250 MB
RAM: Minimum 1 GB, ideal 2 GB+
CPU: Any x68 or x64

Importante: O BluePex® Endpoint Protection pode ser instalado no Servidores Windows. Sem custo adicional.

Controle Avançado de Endpoint e Servidores

BluePex® Endpoint Control

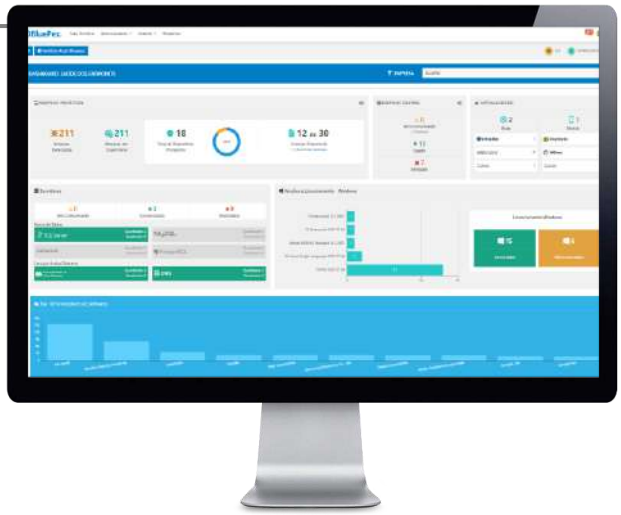
Automatize o inventário de software e hardware de toda sua infraestrutura de rede de modo simples, organizado, centralizado e automático. Controle único de cada dispositivos cadastrado.

GERENCIAMENTO CENTRALIZADA EM NUVEM

Gerenciamento em nuvem que permite gerenciamento de políticas, por grupo ou território, gerência granular com gerenciamento de políticas por nível hierárquico, além de controle de uma ou mais unidades organizacionais. Gerencie a

segurança dos endpoints, dispositivos móveis e servidores de arquivos remotamente, em tempo real, de onde estiver, com o BluePex® Cloud Suite.

MONITORAMENTO EM TEMPO REAL E REMOTO



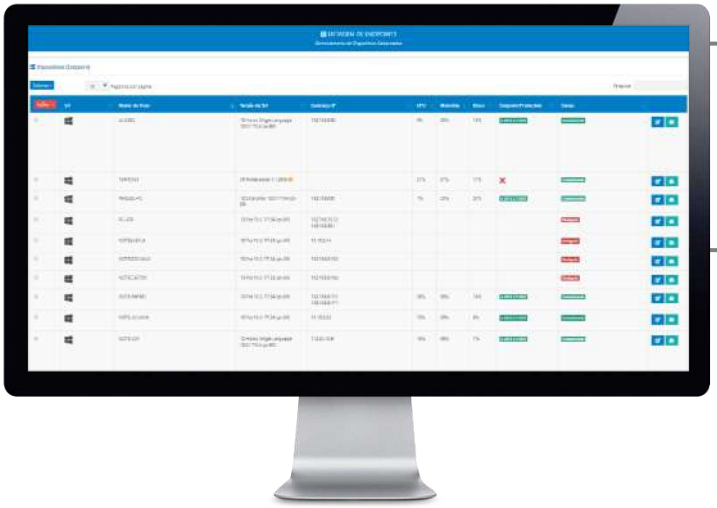
Não espere que um usuário final relate um problema com um ativo de TI, o BluePex® Endpoint Control detecta imediatamente tipos específicos de eventos.

Saiba o que acontece na sua rede e gerencie em tempo real.

- ✓ Segmentação da rede: Sistema operacional, versão do sistema operacional, endereço de IP, CPU, memória e disco, por Endpoint;
- ✓ Gerenciamento de licenças do Windows, número de licenças e condição da licença;
- ✓ Nome de usuário logado no sistema operacional
- ✓ Relatórios de inventário
- ✓ Monitoramento de servidores
- ✓ Monitoramento de banco de dados
- ✓ Monitoramento e estatísticas de virtualizadores instalados na rede
- ✓ Acesso remoto a estações Windows 7 e 10
- ✓ Remoção remota de aplicativos
- ✓ Controle de antivírus instalado por Endpoint;
- ✓ Execute de forma remota escaneamento de Anti Malware por Endpoint;
- ✓ Execute operações remotas como desligar e reiniciar dispositivos;
- ✓ Saiba o local de todos os dispositivos pelo monitoramento por geolocalização, inclusive notebook (laptops);
- ✓ Monitoramento 24 x 7 x 365;

FÁCIL GESTÃO ADMINISTRATIVA DE POLÍTICAS DE ACESSO/PERMISSÕES

Simples e rápido definir políticas gerais como permissões de conexão, acesso restrito por usuário, é possivel criar regras de acesso, por horário, dias e ip.



ANTECIPE PROBLEMAS TÉCNICOS

Com a informação nas suas mãos, será possível prever diversos problemas que podem surgir de atualizações de software, falta de armazenamento, aumento da vida útil dos equipamentos, redução de custos e aumento de produtividade.

NOTIFICAÇÕES SOBRE SERVIÇOS DE REDE

Certifique-se de que seus dispositivos de rede estejam sempre disponíveis e receba notificações imediatas em caso de falhas. Acesse os gráficos de fácil leitura, em tempo real, dos ativos monitorados.

BluePex® Endpoint Protection x Endpoint Control

Características	BluePex® Endpoint Protection	BluePex® Endpoint Control
Detectando e Removendo Malware	✓	
Prevenindo Novos Malware (por comportamento)	✓	
Proteção de Navegação	✓	
Proteção de Arquivos	✓	
Anti-Ransomware	✓	
Alertas e Notificações	✓	✓
Gerenciamento Centralizado em nuvem	✓	✓
Dashboard com informações de ameaças, máquinas protegidas	✓	
Relatórios de ameaças encontradas	✓	
Execute de forma remota escaneamento de Anti-Malware por end-point	✓	
Instalar/desistalar/atualizar Antimalware remotamente de todas as máquinas cadastradas	✓	
Comandos remotos na estação, reiniciar dispositivo e ou desligar dispositivo		✓
Gerenciamento de ativos		✓
Monitoramento de vulnerabilidades em tempo real		✓
Fácil Gestão Administrativa de Políticas de Acesso/Permissões	✓	✓
Acesso Remoto de Todos os Ativos em Rede		✓
Visualize informações detalhadas de cada dispositivo		✓
Descubra tudo que está instalado na sua rede e você desconhece		✓
Proteção Avançada para todas as estações de rede	✓	
Reduz a exposição aos ataques, fortalecendo os endpoints	✓	
Proteja os funcionários externos por gerenciamento remoto	✓	
Monitore os funcionários externos por gerenciamento remoto		✓
Antecipe problemas técnicos, com as informações em mãos		✓
Inventário de software e Hardware		✓
Acesso remoto a estações Windows 7 e 10		✓
Remoção remota de aplicativos		✓
Monitoramento de servidores/banco de dados (SQL,MySQL,etc)		✓
Monitoramento de serviços com DNS e Active Directiory		✓
Gerenciamento de Licenças do Windows, número de licenças e condição da licença		✓
Nome de usuário logado no sistema operacional		✓
Monitoramento de dispositivos, CPU, memória, Disco, serviços, etc.		✓
Monitoramento por geolocalização, inclusive notebook (laptops);	✓	✓
Relatórios de Inventários		✓
Monitoramento 24 x 7 x 365	✓	✓
Suporte ilimitado	✓	✓

- Solução integrada ou isolada - stand alone;
- Integração uma única solução corporativa;
- Acesso em nuvem (Cloud) seguro via HTTPS;
- Soluções em língua portuguesa do Brasil e inglês;
- Regras das políticas em ambiente fora de produção;
- Regras de funcionamento dos bloqueios comportamentais do antivírus, alertas ativos, passivos e silenciosos e automação de açoes mediante alertas:
- Tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- Lista branca e negra com análise de arquivos, bloqueio de aplicações com notificaçõa ativa ou passiva em português do Brasil;
- Proteção de arquivos através de assinaturas de arquivos maliciosos já conhecidos e ativação ou não de proteção quanto PUP do acrônico em inglês Possible Unintended Programs, ou seja, programas possivelmente indesejados como exemplos Adwares e Spywares.;
- Proteção de navegação e proteção quanto a sites maliciosos com base própria, sites com conteúdos indesejados (PUP - Possible Unintended Programs), bem como a inclusão manual pelo administrador de sites na lista branca bem como na lista negra.
- Agendamento de scan na rede, podendo criar mais do que uma regra de agendamento como, por exemplo, um agendamento de scan rápido em um determinado horário do dia e um agendamento completo durante a noite, tecnologia de identificação de condição de carga do equipamento para o scan ser colocado em segundo plano evitando aplicar lentidão ao equipamento, configuração para ocorrer ou não em cada tarefa de agendamento de scan, o agendamento permite frequência diária, semana e mensal, bem como o horário para execução,
- Acesso remoto ao equipamento direto do painel cloud com fator de autenticação adicional;
- Remoção de software remotamente direto do painel cloud
- Ative ou desative recebimento de alertas dos dispositivos;
- Bloqueio de pendrive ou storage externo de forma granular;
- Configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, MEMÓRIA e DISCO e tais informação ficam disponíveis em um painel (dash board) especifico para monitoramento;
- Informações de cada dispositivo:
  - ✓ Status do Dispositivo;
  - ✓ Data em que os dados foram coletados;
  - ✓ O número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo;
  - ✓ Nome do Host;
  - ✓ Versão do antivirus/antimalware;
  - ✓ Versão do Sistema Operacional;
  - ✓ Usuário logado no dispositivo;
  - ✓ Tempo de Atividade;
  - ✓ Consumo e total de CPU;
  - ✓ Consumo e total de memória RAM;
  - ✓ Consumo e total de memória Swap;
  - ✓ Consumo e volume total de Disco;
  - ✓ Interfaces de rede;
  - ✓ Serviços que estão em execução;
  - ✓ Serviços que estão parados;
  - ✓ Processos que estão mais consumindo CPU;
  - ✓ Processos que estão mais consumindo Memória;
  - ✓ Hardware: Drivers de impressora, CD-ROM, Dispositivos gerais, IDE, USB, SOM, VÍDEO, Adaptador de Rede, Processaor, BIOS, MEMÓRIA, PLACA DE SOM, DISCO, MEMÓRIA.
  - ✓ Softwares instalados: fabricantes, software e versão;
- Gerenciamento Web possui Dashboard com informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- Dashboard detalhado do gerenciamento do antimaware, monitoramento e inventário de rede com estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, dispositivos ligados, desligados, monitoramento de servidores, monitoramento de banco de dados SQLServer, MySQL, PostgreSQL, Oracle, monitoramento Microsoft Active Directory e DNS, de sistemas operacionais instalados, versão do sistema operacional, máquinas com licença ativa do Windows e licenças não validas, vencidas, sem licença e resumo dos 10 maiores fornecedores de software;
- Painel de visualização com cores e com informações

básicas de quais dispositivos estão com problemas, alertas e quais estão com execução sem nenhum problema;

- Relatórios de informações extraídas dos dispositivos, relatórios de inventário de software e hardware, relatórios de equipamentos e licença do Windows e seu status, software virtualizado instalado, relatório de licença do antimalware e suas aplicações, relatório de infecções e equipamentos infectados, nome da infecção e nível de risco da mesma.
- Atende sistemas operacionais da família Windows da versão Windows 7 e servidores Windows server 2008 R2 em diante.
- Agente para monitoramento dos sistemas operacional Linux prevendo o funcionamento nas versões CentOs 7 e 7, Debian 8, 9 e 10, Ubunto 14, 16 e 18;
- Monitoramento dos agentes em Linux: Ativar ou desativar recebimento de alerta dos dispositivos e configuração de tipos de alertas, monitoramento dos dispositivos: percentuais de CPU, MEMÓRIA e DISCO e estão disponíveis em um painel ou Dash Board específico para monitoramento;
- Informações de cada dispositivo:

✓ Status do Dispositivo;
✓ Data em que os dados foram coletados;
✓ Nome do Host;
✓ Versão do Sistema Operacional;
✓ Usuário logado no dispositivo;
✓ Consumo e total de CPU;
✓ Consumo e total de memória RAM;
✓ Consumo e total de memória Swap;
✓ Consumo e volume total de Disco e suas partições;
✓ Interfaces de rede;
✓ Serviços que estão em execução;
✓ Serviços que estão parados;
✓ Processos que estão mais consumindo CPU;
✓ Processos que estão mais consumindo Memória;
✓ Histórico de comandos executados;
✓ Localização do dispositivo em mapa georreferenciado;

✓ Configuração de serviços e o agente que irá monitorar, em caso de parada do serviço o agente reinicia o mesmo;

- Relatórios de inventário de software e hardware, relatório de licenças do Windows com seu status e relatórios de ameaças encontradas, os relatórios são gerados no formato PDF, CSV e HTML
- Proteção oferecida

✓ Proteção contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes (“worms”), cavalos de tróia (“trojan”), códigos espiões (“spyware”, “keylogger”, “screenlogger”, etc), códigos de apoio à invasão e escalada de privilégio (“rootkit”, “backdoor”, etc), código e conteúdo indesejado (“dialer”, “adware”, “joke”,etc);

✓ Rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho.

✓ Negação de acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware, limpeza de arquivo, e/ou delete do arquivo infectado e envio do arquivo infectado para uma área de segurança (quarentena).

✓ Proteção de mídias removíveis (“CD”, “DVD”, “pendrive”, “HD” externo), sem a necessidade de configurações adicionais.

✓ Detecção de ameaças em arquivos compactados nos principais algoritmos (“ZIP”, “RAR”, “7zip”)

✓ Proteção de tempo real com listas brancas (whitelist) adicão de arquivo em específico ou um diretório, permitindo todos os arquivos a serem executados e recursivamente.

✓ Execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
✓ Sistema avançado de limpeza que reduz o risco de estabilidade do sistema operacional;
✓ Camada de proteção contra acesso a sites fraudulentos e perigosos;
✓ Camada de proteção de arquivos contra sequestro de informações;

✓ Camada de proteção comportamental contra programas e/ou comportamentos suspeitos;

✓ Módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;

✓ Kit de emergência para usuário dar boot na máquina e limpeza manual;

✓ Bloqueio por meio de comportamento dos processos, sistemas e programas;

BluePex®

O que nos torna únicos

Simples, Fácil e Intuitivo

A BluePex® desenvolve as soluções pensando na experiência do cliente, nosso foco é manter uma linha de soluções simples e segura. A BluePex® se renova diariamente na busca por novas tecnologias e melhores soluções. Também atendemos necessidades exclusivas de cada cliente criando novos features.

Desenvolvimento Próprio

O Brasil tem suas peculiaridades e nós conhecemos como ninguém! Nossas soluções são projetadas para a realidade nacional. Temos expertise mundial, contamos com parceiros estratégicos em várias partes do mundo, tornando-nos mais fortes. Inovação é o que nos move.

Portfólio Completo de Segurança e Controle com Soluções em Nuvem

Tenha em um único fornecedor as principais soluções para Controle e Segurança da Informação: Advanced Mail Security, Next-Generation Firewall, Website Security, Endpoint Protection, Endpoint Control, Datacenter Watch (IoT) e Data Recovery Solutions.

SaaS

Saas (Software como Serviço) permite aos usuários se conectar e usar aplicativos baseados em nuvem pela internet, baixo custo inicial, maior capacidade para adaptação, acesso de qualquer lugar.