kaspersky

Enhanced Support e Enhanced Support with TAM

Programas de suporte técnico estendido para proprietários de licenças “Plus”

kaspersky

1. Termos e condições gerais

A Kaspersky fornecerá suporte técnico estendido aos proprietários de certificados dos programas de Enhanced Support ou Enhanced Support with TAM em relação aos casos de suporte técnico contidos na lista apresentada neste documento.

O objetivo destes programas é proporcionar ao Usuário final que possui a licença “Plus” de produtos da Kaspersky e um dos certificados com suporte técnico de qualidade superior em relação aos termos do Suporte técnico padrão fornecido de acordo com o Contrato de Licença de Usuário Final da Kaspersky, que determina os termos de utilização do Produto de software pelo Usuário final.

2. Definições

“Company Account” refere-se ao sistema de processamento de solicitações de suporte técnico na Web da Kaspersky.

“Produto(s)” refere-se aos produtos de software da Kaspersky comprados pelo Cliente, implementados e instalados em conformidade com os termos de um Contrato de Licença entre a Kaspersky e o Cliente, e para os quais o Cliente firmou um Contrato de Licença.

“Usuário Final”, **“Usuário”**, **“Cliente”, (Você/Seu)** refere-se a uma organização que tem uma licença “Plus” do Produto em vigor, que inclui suporte em conformidade com este Programa.

“Incidente” refere-se a cada evento informado pelo Cliente e que não faz parte do funcionamento padrão de um Produto e que causa ou pode causar uma interrupção ou redução na qualidade do serviço fornecido pelo Produto.

“Horário local” refere-se ao fuso horário do Escritório local da Kaspersky.

“Problema” refere-se a uma causa subjacente desconhecida de um ou mais Incidentes. Ele se torna um Erro conhecido quando a causa básica é conhecida e foi identificada uma opção temporária ou uma alternativa permanente.

“Erro conhecido” refere-se a um Problema que se torna um Erro conhecido quando a causa básica é conhecida e foi identificada uma opção temporária ou uma alternativa permanente.

“Erro do produto” refere-se ao comportamento não declarado do Produto.

“Solicitação de serviço” refere-se a uma solicitação de suporte, entrega, informações, consultoria ou documentação feita pelo Cliente e que não está relacionada ao funcionamento incorreto ou ao não funcionamento do(s) Produto(s).

“Surto de vírus” refere-se a uma situação de crise para o Cliente, na qual um vírus não detectado pelo(s) Produto(s) com os bancos de dados de antivírus e os módulos executáveis mais recentes afeta a continuidade dos negócios e/ou um grande número de usuários finais do Cliente. O Surto de vírus é um Incidente relacionado ao produto.

“Incidente relacionado a malware/incidente com vírus” refere-se a um Incidente não relacionado ao produto que requer instruções da Kaspersky sobre a remoção de um malware específico e/ou descrições de malware e/ou ferramentas específicas de remoção de malware.

“Gravidade/urgência do incidente” refere-se a uma medida da gravidade de um incidente ou problema para os negócios com base nas necessidades comerciais do Cliente. Veja mais detalhes no Apêndice.

“Tempo de resposta” refere-se ao tempo decorrido entre o momento do recebimento de um incidente até a resposta apropriada ao solicitante (via sistema de suporte, e-mail ou telefone).

“Atualização” refere-se aos bancos de dados de antivírus distribuídos pela Kaspersky com novas assinaturas de vírus ou modificações dos módulos executáveis do Produto que melhoram seu desempenho e/ou ampliam sua funcionalidade.

“Upgrade” refere-se às atualizações do Produto associadas à atribuição de um novo número de versão.

“Alternativa” refere-se a um procedimento que pode servir como solução temporária para um incidente.

“Alarme falso”, **“Falso positivo”** refere-se a uma situação em que o Produto detecta incorretamente um arquivo seguro como infectado.

kaspersky

3. Descrição dos programas

O suporte técnico relacionado ao funcionamento do produto, assim como o recebimento de solicitações de manutenção pós-incidentes, é implementado por meio de:

- Portal Web de suporte técnico da Kaspersky, que recebe solicitações 24 horas por dia, 365 dias por ano
- Linha telefônica prioritária 24 horas por dia, 365 dias por ano;
- Gerente técnico da conta designado, durante o horário comercial no horário local (para proprietários do certificado de Enhanced Support with TAM)

Processamento de incidentes

Processamento de incidentes via painel da Company Account na Web

O sistema de processamento de solicitações de Suporte técnico da Kaspersky na Web está disponível em: https://companyaccount.kaspersky.com

Nesse sistema, o Cliente pode tirar proveito de:

- acesso a sua conta pessoal a fim de criar, atualizar e monitorar incidentes;
- suporte técnico e consultoria relacionados a incidentes que podem ocorrer durante a instalação, configuração e funcionamento do Produto;
- recebimento de recomendações para desinfetar computadores infectados por malware.

Processamento de incidentes por telefone

O Suporte técnico por telefone está disponível somente aos contatos autorizados do Cliente.

Tempos de resposta

A Kaspersky garante os seguintes tempos de resposta, dependendo da urgência da solicitação do cliente e do nível do certificado do programa de suporte estendido. Solicitações de clientes de nível 1 (para o programa de Suporte avançado) e de nível 1 e 2 (para o programa de Suporte avançado com TAM) serão processadas 24 horas por dia, 365 dias por ano:

Nível de gravidade	Enhanced Support	Enhanced Support with TAM
Nível 1	2 horas*	30 minutos*
Nível 2	6 horas úteis	4 horas*
Nível 3	8 horas úteis	6 horas úteis
Nível 4	10 horas úteis	8 horas úteis

*Para obter o tempo de resposta garantido para sua solicitação durante o horário não comercial, reproduza sua solicitação por telefone.

As solicitações de clientes dos programas de Enhanced Support são atribuídas com prioridade maior que as solicitações do pacote de suporte padrão. Quando necessário, os Especialistas em suporte técnico podem solicitar uma sessão remota com o cliente para acelerar a resolução do incidente.

O nível de urgência é determinado pela categoria escolhida pelo cliente (na lista suspensa disponível na Conta da empresa) ao entrar em contato com o Suporte técnico e pela natureza do incidente. A Kaspersky se reserva o direito de alterar o nível de urgência da solicitação, caso a gravidade do caso especificada pelo cliente não se confirme. A lista de níveis de urgência com suas descrições é fornecida no Apêndice.

kaspersky

Controle de resolução de incidentes

A qualquer momento, um incidente pode estar no lado do Cliente (ou seja, o Cliente está tomando medidas que vão promover/acelerar a resolução do problema pela Kaspersky) ou no lado da Kaspersky.

Um incidente encontra-se no lado do Cliente quando a Kaspersky solicita informações do Cliente. Quando o Cliente fornece as informações solicitadas à Kaspersky, é considerado que o Incidente está no lado da Kaspersky. O período durante o qual o incidente pode ficar no lado do Cliente limita-se a 1 mês. Caso a resposta do Cliente atrase, o incidente será encerrado por ter atingido o tempo limite.

A Kaspersky é responsável somente pelo tempo durante o qual o incidente está em seu lado.

Benefícios adicionais do programa de Enhanced Support with TAM

Gerente técnico da conta (TAM) exclusivo

O Gerente técnico da conta (TAM) é um funcionário da Kaspersky designado para o cliente com o objetivo de manter um canal de comunicação integrado. Ele gerencia o processamento de todas as solicitações do cliente. As responsabilidades do Gerente técnico da conta são estabelecidas da seguinte maneira:

- organização da comunicação para o processamento de incidentes pelas equipes técnicas da Kaspersky;
- notificação do Cliente sobre o status atual dos incidentes; fornecimento de relatórios trimestrais;
- supervisão do andamento de tarefas relacionadas às solicitações do Cliente e implementação de encaminhamentos rápidos ao processar solicitações;
- suporte ao departamento de TI do Cliente em relação a recomendações e instruções fornecidas pelos especialistas da Kaspersky;
- trabalho analítico em colaboração com o Cliente a fim de resolver os incidentes técnicos e operacionais atuais.
- processamento de dúvidas relacionadas a detecções repetidas de malware quando o endpoint é capaz de detectar e evitar atividade maliciosa, mas o usuário continua recebendo alertas de infecção por malware.

O TAM fica disponível durante o horário comercial e no horário do escritório local da Kaspersky por telefone fixo, celular e e-mail. Se o TAM não estiver disponível (fora do horário comercial, incluindo fins de semana), as solicitações do Cliente serão direcionadas ao gerente de plantão na linha de Suporte técnico MSA. O horário comercial pode variar de acordo com a região. Confira os detalhes em seu certificado.

O Cliente deve designar contatos (de acordo com os Termos adicionais de suporte) para a comunicação com a Kaspersky e fornecer à Kaspersky seus detalhes de contato (e-mail, telefone e outros, se disponíveis) para possibilitar a colaboração consistente e eficiente relacionada à resolução de incidentes.

Verificação remota da integridade

Clientes com o certificado de Enhanced Support with TAM têm direito a 8 horas de serviço remoto de verificação de integridade durante a vigência do certificado.

Encaminhamento de incidentes e gerenciamento de reclamações

Reclamações referentes à qualidade do suporte técnico são aceitas de acordo com o seguinte esquema:

Nível de encaminhamento	1	2	3
	Gerente técnico da conta	Chefe da equipe de suporte, escritório local da Kaspersky	Gerente comercial da conta (Contato comercial)

O Cliente poderá encaminhar incidentes não resolvidos, caso estejam no lado da Kaspersky.

kaspersky

Fornecimento de relatórios sobre incidentes abertos

Durante o processo de resolução de incidentes, a Kaspersky se empenhará ao máximo em fornecer imediatamente ao Cliente informações sobre o status dos incidentes abertos de acordo com a seguinte tabela.

Nível de gravidade	Programação de comunicação
Nível 1	De acordo ao combinado, mas não mais do que uma vez ao dia (por e-mail ou telefone)
Nível 2	Dentro dos relatórios regulares
Nível 3	
Nível 4	

Lançamento do banco de dados de antivírus por solicitação de clientes no caso de incidente de malware ou falso positivo

Caso ocorra um falso negativo (quando um arquivo infectado é identificado pelo Produto como seguro) ou, ao contrário, um falso positivo, desde que sejam utilizados os bancos de dados de antivírus mais recentes, o Cliente pode solicitar a alteração das assinaturas de vírus do Produto. A Kaspersky fornecerá a atualização do Produto que garantirá a detecção correta do arquivo ao Cliente.

A Kaspersky implementa as seguintes atividades:

- Processamento de solicitações referentes ao lançamento de bancos de dados de antivírus (realizado por um grupo exclusivo de especialistas que trabalha em modo 24/7/365)
- Lançamento de atualizações de alta prioridade (expresso) para proprietários do certificado de Enhanced Support with TAM.
- Informação do Cliente sobre o andamento de suas solicitações pelo Gerente técnico da conta.

Fornecimento de correções públicas e privadas

- Processamento de solicitações referentes ao lançamento de patches e correções privadas (realizadas por um grupo de engenheiros dedicado às solicitações dos assinantes)
- Informação do Cliente sobre o andamento de suas solicitações pelo Gerente técnico da conta

A Kaspersky se empenhará de modo comercialmente racional para lançar um código privado de correção do programa (patch privado). Os códigos de correção do programa são lançados de acordo com a divisão do ciclo de vida de suporte do produto contida nos Termos e condições dos Serviços de suporte (a versão atualizada está disponível em: https://support.kaspersky.com/support/rules#en_us).

Os termos de uso das correções privadas do programa são tratados no Contrato de licença entre a Kaspersky e o Cliente.

Termos adicionais de suporte

O Cliente com certificado de Enhanced Support pode designar até 4 (quatro) contatos autorizados a abrir solicitações para o Suporte técnico da Kaspersky.

O Cliente com certificado de Enhanced Support with TAM pode designar até 8 (oito) contatos autorizados a abrir solicitações para o Suporte técnico da Kaspersky.

Uma lista de contatos autorizados deve ser definida no certificado fornecido pela equipe de suporte da Kaspersky. Para alterar a lista de contatos autorizados, o Cliente deve enviar uma solicitação por escrito via portal Web. A Kaspersky fornecerá uma versão atualizada do certificado ao Cliente.

O Cliente pode registrar um número ilimitado de incidentes durante a validade do certificado de Enhanced Support e Enhanced Support with TAM.

Alguns incidentes podem exigir a reprodução pela Kaspersky com a finalidade de testar e verificar uma infecção por vírus ou um erro do produto.

O Cliente deve fornecer à Kaspersky todas as informações necessárias e o software ou hardware específicos que possam ser necessários para a reprodução das condições em que o incidente será repetido e poderá ser examinado. Isso poderá ser necessário se a Kaspersky não tiver o software ou hardware necessários disponíveis.

A Kaspersky se esforçará para reproduzir o incidente assim que todas as informações e o software e/ou hardware necessários forem fornecidos.

Se não for possível reproduzir o incidente, o Cliente deverá permitir que os especialistas da Kaspersky tenham acesso remoto supervisionado ao sistema com avarias.

Se alguma das partes não conseguir reproduzir o incidente ou se o Cliente não permitir o acesso ao ambiente de rede no qual o incidente poderia ser reproduzido ou se for estabelecido que a causa do incidente não está relacionada ao Produto, o incidente não poderá ser classificado dentro deste Programa de suporte.

Limitações dos programas de suporte técnico estendido: Enhanced Support e Enhanced Support with TAM

O suporte técnico incluído nos programas Enhanced Support e Enhanced Support with TAM não deverá ser implementado no caso dos seguintes incidentes:

- incidentes já resolvidos para o Cliente (ou seja, incidentes que ocorreram em uma cópia instalada do Produto depois que o mesmo incidente já foi resolvido para outra cópia do Produto);
- solução de problemas semelhantes ou idênticos a problemas já resolvidos (ou seja, incidentes aos quais uma solução produzida anteriormente pode ser aplicada sem orientação adicional da Kaspersky);
- incidentes causados por avarias no hardware do Cliente;
- incidentes causados por incompatibilidade da plataforma de software (incluindo, mas não se limitando a software beta, novas versões de service packs ou adições cuja compatibilidade com o Produto não foi confirmada pela Kaspersky);
- incidentes causados pela instalação e execução de aplicativos de terceiros (incluindo, mas não se limitando à lista de aplicativos sem suporte ou incompatíveis publicada na documentação);
- incidentes sobre os quais o Cliente não é capaz de fornecer informações precisas conforme solicitação cabível da Kaspersky a fim de reproduzir, investigar e resolver o incidente;
- incidentes decorrentes de negligência ou uso incorreto de instruções da Kaspersky que, se utilizadas corretamente, teriam claramente evitado o incidente.

Apêndice

Níveis de gravidade de incidentes com o produto

“Nível de gravidade 1” (crítico) refere-se a um problema crítico com o Produto que afeta a continuidade dos negócios do Cliente com interrupções no funcionamento normal do Produto e que causa o travamento do(s) Produto(s) ou do Sistema operacional, ou que causa perda de dados, alteração das configurações padrão para valores inseguros, ou problemas de segurança, desde que não haja uma Alternativa disponível.

A lista de incidentes relacionados ao Produto que correspondem ao Nível de gravidade 1 inclui, mas não se limita aos seguintes problemas:

- toda a rede local (ou sua parte essencial) está inoperante, o que dificulta ou impossibilita os principais processos de negócios.

“Nível de gravidade 2” (alto) refere-se a um problema moderado que afeta a funcionalidade do produto, mas não causa corrupção/perda de dados ou travamento do software. O Nível de gravidade 1 é reclassificado para o Nível de gravidade 2 quando há uma alternativa disponível.

A lista de incidentes relacionados ao Produto que correspondem ao Nível de gravidade 2 inclui, mas não se limita aos seguintes problemas:

- o produto não funciona corretamente ou não funciona, mas a continuidade dos principais processos de negócios não é interrompida.

“Nível de gravidade 3” (médio) refere-se a um problema ou uma solicitação de serviço não críticos e que não afetam a funcionalidade do Produto.

A lista de incidentes que correspondem ao Nível de gravidade 3 inclui, mas não se limita aos seguintes problemas:

- o produto está parcialmente inoperante (não funciona corretamente), mas sem envolvimento de outros aplicativos utilizados pelo Cliente.

“Nível de gravidade 4” (baixo) refere-se a outros problemas ou solicitações de serviço não críticos. Todos os incidentes que não atendem aos critérios relacionados acima correspondem a esse nível de gravidade.

Níveis de gravidade de incidentes com vírus

“Nível de gravidade 1” (crítico) refere-se a surtos de vírus que afetam a continuidade dos negócios do Cliente com interrupções no funcionamento normal do Produto e que causam o travamento do(s) Produto(s) ou do sistema operacional, ou que causam perda de dados, desde que não haja uma Alternativa disponível.

A lista de incidentes relacionados a malware que correspondem ao Nível de gravidade 1 inclui, mas não se limita aos seguintes problemas:

- toda a rede local (ou sua parte essencial) está inoperante;
- surtos de vírus;
- falsos positivos para arquivos que referem-se a sistemas essenciais para os negócios.

“Nível de gravidade 2” (alto) refere-se a um problema moderado que afeta a funcionalidade do produto, mas não causa corrupção/perda de dados ou travamento do software. O Nível de gravidade 1 é reclassificado para o Nível de gravidade 2 quando há uma alternativa disponível.

A lista de incidentes relacionados a malware que correspondem ao Nível de gravidade 2 inclui, mas não se limita aos seguintes problemas:

- infecção de alguns nós não críticos da rede;
- falsos positivos para arquivos que não se referem a sistemas essenciais para os negócios.

www.kaspersky.com.br/
www.securelist.com