Email Security.cloud da Symantec

Descrição de Serviço

Setembro de 2018

Esta Descrição de Serviço descreve o Email Security.cloud ("Serviço") da Symantec. Todos os termos em letras maiúsculas desta descrição têm o significado atribuído a eles no Contrato (definido abaixo) ou na seção Definições.

Esta Descrição de Serviço e quaisquer anexos incluídos para referência são incorporados ao contrato assinado manual ou digitalmente pelo Cliente com a Symantec, ou fazem parte dele. Se não houver um contrato assinado, ele será regido pelos Termos e Condições dos Serviços online da Symantec (doravante referidos como o "Contrato").

Sumário

1: Recursos e funcionalidades técnicas e comerciais

- Visão geral do Serviço
- Recursos e opções do Serviço
- Contrato de Nível de Serviço
- Plataformas compatíveis e requisitos técnicos
- Componentes de software dos serviços hospedados

2: Responsabilidades do Cliente

- Política de uso aceitável

3: Informações sobre assinatura e direitos

- Métricas de cobrança
- Mudanças na assinatura

4: Assistência e suporte técnico

- Assistência ao cliente
- Suporte técnico
- Manutenção para o Serviço e/ou suporte de Infraestrutura de Serviço

5: Termos adicionais

6: Definições

Anexo A Contrato de Nível de Serviço

Email Security.cloud da Symantec

Descrição de Serviço

Setembro de 2018

1: Recursos e funcionalidades técnicas e comerciais

Visão geral do Serviço

O Symantec™ Email Security.cloud é um serviço hospedado que filtra mensagens de Email e ajuda a proteger empresas contra malware (incluindo ataques direcionados e phishing), spam e Emails em massa indesejáveis. O Serviço oferece opções de criptografia e proteção de dados para ajudar a controlar as informações confidenciais enviadas por Email. O Serviço oferece suporte a vários tipos de caixas de correio de diferentes fornecedores.

Recursos do Serviço

- Os Administradores do Cliente podem acessar o console de gerenciamento do Serviço usando um login seguro protegido por senha. O console de gerenciamento permite que o Cliente configure e gerencie o Serviço, acesse relatórios e visualize os dados e as estatísticas quando estiverem disponíveis como parte do Serviço.
- O Serviço é gerenciado 24 horas por dia, 7 dias por semana, e monitora a disponibilidade do hardware, a capacidade do serviço e a utilização dos recursos de rede. A conformidade dos níveis do serviço é monitorada regularmente no Serviço, e os ajustes são feitos conforme necessário.
- A geração de relatórios para o Serviço está disponível por meio do console de gerenciamento. Os relatórios poderão incluir logs de atividades e/ou as estatísticas. No console de gerenciamento, o Cliente pode gerar relatórios, que podem ser configurados para serem enviados por Emails agendados ou obtidos por download por meio desse console.
- O Serviço tem o objetivo de permitir que o Cliente implemente uma política de uso do computador imposta e válida ou equivalente.
- As listas de palavras e regras de modelos sugeridas ou as políticas fornecidas pela Symantec contêm palavras que podem ser consideradas ofensivas.
- Caso o Serviço seja suspenso ou encerrado por qualquer motivo, a Symantec poderá reverter todas as alterações de configuração feitas no provisionamento do Serviço. Será responsabilidade do Cliente realizar todas as outras alterações necessárias à configuração caso o Serviço seja restabelecido.

Recursos e opções do Serviço

Duas (2) opções do Serviço estão disponíveis: Email Protect ou Email Safeguard. O Serviço deve ser adquirido para cada Usuário da opção ou complemento selecionado (sujeito a todas as restrições explicadas nesta Descrição de Serviço).

Recursos por opção de serviço

	Email Protect	Email Safeguard
Antimalware para Email: proteção antimalware que inclui proteção contra phishing e ataques direcionados	✓	✓
Antispam para Emails: proteção contra spam, phishing (com acompanhamento de links em tempo real) e Email em massa	✓	✓
Email Data Protection controles personalizáveis para políticas de filtragem de conteúdo		✓
Email Image Control: Detecção de imagens ofensivas		✓

Filtragem de emails de saída	✓	✓
Criptografia TLS imposta		✓
Criptografia TLS oportunista	✓	✓
Registro de endereços: administração inválida de destinatários	✓	✓
Ferramenta de Sincronização LDAP para usuários e grupos	✓	✓
Rastreamento de mensagens	✓	✓
Painel de relatórios	✓	✓
Relatórios de resumo (PDF) e detalhados (CSV)	✓	✓
Notificações e portal de quarentena do spam do usuário final	✓	✓
Gerenciamento de isenções de responsabilidade	✓	✓
Policy Based Encryption Essentials		✓
Controles de representação de email		✓

Para obter mais informações sobre recursos individuais de serviço, acesse a ajuda online em http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=PT_BR.

Complementos do serviço

	Email Protect	Email Safeguard
Advanced Threat Protection: Email	Disponível	Disponível
Policy Based Encryption Advanced	_	Disponível
Email Fraud Protection	Disponível	Disponível
Email Threat Isolation	Disponível	Disponível

Para obter mais informações sobre complementos individuais de serviço, acesse a ajuda online em http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=PT_BR. A Descrição de Serviço do Email Fraud Protection pode ser encontrada em: https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: o Email detecta ameaças avançadas enviadas por Email usando a área restrita do Symantec Cynic™, identifica ataques direcionados por Email contra a empresa ou usuário-alvo e identifica URLs que se tornam maliciosos após a entrega de Emails, com Symantec Click-time™ URL Protection. Ele pode obter emails que são considerados maliciosos depois da entrega por nossa área restrita do Cynic™ para clientes do O365. Ele fornece relatórios detalhados de malwares, incluindo informações sobre URL, categoria do malware, método de detecção e hashes de

arquivos. Uma API de feed de dados é incluída para permitir a geração de relatórios de malware por meio de um URL autenticado, sem que seja necessário importar arquivos ou enviar dados por email. Advanced Threat Protection: O Email também dá acesso ao serviço Phishing Readiness, um simulador de ataque de phishing usado para identificar se os funcionários estão suscetíveis a esse tipo de ataque. O uso do serviço Phishing Readiness é regido pelos termos e pelas condições em (https://www.symantec.com/about/legal/repository).

O Policy Based Encryption Advanced oferece: (i) um portal de coleta na Web; (ii) suporte à entrega via PGP e S/MIME; (iii) recurso para tentar realizar a criptografia TLS antes de utilizar tecnologias de criptografia menos transparentes e (iv) uma entrega por envio de um .pdf criptografado (o único método de criptografia fornecido como parte do recurso Policy Based Encryption Essentials no plano Email Safeguard). O Policy Based Encryption Advanced é licenciado por usuário-remetente, que pode ser um subconjunto da contagem de usuários total para a opção Email Safeguard. Se o Cliente exigir o uso da opção Policy Based Encryption Advanced para a entrega segura de declarações, a Symantec poderá permitir que o Cliente compre licenças de usuário adicionais, com base na quantidade de declarações a serem entregues, de acordo com uma fórmula definida pela Symantec.

O Symantec™ Email Fraud Protection é um serviço em nuvem que automatiza a imposição de conformidade, geração de relatórios e autenticação de mensagens baseadas em domínio (DMARC, Domain-Based Message Authentication, Reporting, and Conformance). O Symantec Email Fraud Protection facilita e descomplica ainda mais cada etapa para imposição de DMARC em comparação com o método manual. A imposição reduz o risco de ataques de representação de entrada, pois todos os emails provenientes de fontes não autenticadas são enviados para quarentena ou são rejeitados. Quando estiverem na imposição, os destinatários dos emails ou os Agentes de transferência de mensagens sabem que podem confiar no domínio do cliente, aumentando, assim, as taxas de entrega de emails.

O Symantec™ Email Threat Isolation reforça a proteção contra spear phishing, roubo de credenciais e ataques de email avançados isolando links maliciosos e renderizando com segurança páginas da Web perigosas. O Email Threat Isolation permite que a Symantec ofereça a melhor proteção contra ameaças de email sofisticadas que usam links maliciosos, como o spear phishing avançado ou ataques de roubo de credenciais.

O Email Threat Isolation cria um ambiente de execução seguro entre os usuários e seus links de email, renderizando links suspeitos remotamente e mostrando apenas conteúdo da Web seguro aos usuários. Como resultado, a Symantec impede que ameaças que contenham links maliciosos cheguem até os usuários, já que todo o link recebido é tratado como malicioso e executado remotamente, longe dos usuários e seus dispositivos. O Email Threat Isolation também impede ataques de phishing para roubo de credenciais renderizando os sites de phishing em um modo somente leitura, o que previne que os usuários insiram credenciais corporativas e outras informações credenciais.

Contrato de Nível de Serviço

- A Symantec oferece o Contrato de Nível de Serviço ("SLA", Service Level Agreement) aplicável ao serviço conforme especificado no Anexo A.

Plataformas compatíveis e requisitos técnicos

- Você encontra as plataformas compatíveis e os requisitos técnicos do Serviço em http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=PT_BR.

Componentes de software dos serviços hospedados

- O Serviço inclui os Componentes de Serviço do software disponíveis no console de gerenciamento, que pode ser acessado após o pagamento da taxa aplicável.

2: Responsabilidades do Cliente

A Symantec apenas poderá realizar o Serviço se o Cliente fornecer as informações necessárias ou executar as ações necessárias; do contrário, o desempenho do Serviço da Symantec poderá ser atrasado, prejudicado ou impedido, e/ou a elegibilidade para os benefícios do Contrato de Nível de Serviço poderá ser invalidada conforme indicado abaixo.

- Ativação da configuração: O Cliente deve fornecer as informações necessárias para a Symantec começar a fornecer o Serviço.
- Equipe de atendimento ao Cliente adequada: O Cliente deverá empregar funcionários capacitados para ajudar a Symantec a fornecer o Serviço, de acordo com solicitação viável da Symantec.

- O Cliente é responsável pelas informações, senha ou outras credenciais de login de sua conta.
- O Cliente concorda em usar meios razoáveis para proteger as credenciais e notificará a Symantec imediatamente de qualquer uso não autorizado conhecido da conta do Cliente.
- Credenciais de renovação: se aplicável, o Cliente deverá usar as credenciais de renovação fornecidas no Instrumento de Assinatura aplicável ou na Confirmação do Pedido durante a administração da conta para que continue a receber o Serviço ou para manter as informações da conta e os dados do Cliente que estarão disponíveis durante o período de duração do Serviço.
- Configurações do Cliente e configurações padrão: O Cliente deve configurar os recursos do Serviço por meio do console de gerenciamento, se aplicável. Caso contrário, as configurações padrão serão aplicadas. Em alguns casos, as configurações padrão não existem e nenhum Serviço será fornecido até que o Cliente escolha uma configuração. O Cliente tem poder total de configuração e o uso do(s) Serviço(s); assim, a Symantec não será responsabilizada pelo uso que o Cliente fizer do Serviço, nem responsabilizada por qualquer responsabilidade civil ou criminal incorrida pelo Cliente como consequência da operação do Serviço.

Política de uso aceitável

- O Cliente é responsável por estar em conformidade com a Política de uso aceitável dos Serviços online da Symantec.

3: Informações sobre assinatura e direitos

Métricas de cobrança

O Serviço está disponível sob a seguinte Métrica conforme especificado na Confirmação do Pedido:

- "**Usuário**" é um indivíduo e/ou dispositivo autorizado a usar e/ou aproveitar os benefícios do uso do Serviço, ou que utiliza qualquer parte do Serviço.

Mudanças na assinatura

Se o Cliente tiver recebido o Direito ou Assinatura do Cliente diretamente da Symantec, os comunicados relacionados às alterações permitidas da Assinatura ou Direito do Cliente deverão ser enviados ao seguinte endereço (ou endereço substituto publicado pela Symantec): CLD_cancellations_MLABS@symantec.com ou conforme determinado no Contrato do Cliente com a Symantec. Qualquer aviso fornecido de acordo com esse procedimento será considerado como tendo sido fornecido quando recebido. Se o Cliente tiver recebido a Assinatura ou o Direito do Cliente através de um revendedor da Symantec, entre em contato com esse revendedor.

4: Assistência e suporte técnico

Nota: Esta seção apenas será aplicada se o Cliente for intitulado para receber a Assistência e Suporte ao Cliente diretamente da Symantec ("Suporte"). Se um Cliente tiver direito a receber Assistência e Suporte de um revendedor da Symantec, consulte o contrato do Cliente com o revendedor para obter detalhes sobre esse Suporte. O Suporte descrito no aqui não se aplicará ao Cliente.

Assistência ao cliente

A Symantec fornecerá a assistência abaixo como parte do Serviço durante o horário comercial local:

- Recebimento e processamento de pedidos para implementação do Serviço;
- Receber e processar solicitações para fazer modificações permitidas nos recursos do Serviço; e
- Resposta a perguntas sobre faturas e cobranças.

Suporte técnico

O Suporte a nível de entrada está incluído como parte do Serviço conforme especificado abaixo.

- O Suporte está disponível vinte e quatro (24) horas por dia, sete (7) dias por semana para ajudar o Cliente com a configuração dos recursos do Serviço e para resolver problemas relacionados ao Serviço. O Suporte a Serviços será realizado segundo os termos e condições publicados bem como políticas de suporte técnico publicadas em https://support.symantec.com/pt_BR/article.TECH236428.html.

- Uma vez que um nível de gravidade seja designado a uma submissão do Cliente para Suporte, a Symantec fará todos os esforços razoáveis para responder segundo os objetivos de resposta definidos na tabela abaixo. Falhas resultantes de ações do Cliente ou que exijam ações de outros provedores de serviços estão fora do controle da Symantec e, como tal, são excluídas deste compromisso de Suporte.

Gravidade do problema	**Objetivos de resposta de suporte (24 horas por dia, 7 dias por semana)***
Gravidade 1: Um problema ocorreu para o qual não há uma solução alternativa que possa ser aplicada imediatamente em uma das seguintes situações: (i) o servidor de produção do Cliente ou outro sistema de grande importância está inativo ou teve uma perda substancial de serviço ou (ii) uma quantidade significativa de dados importantes do Cliente está em alto risco de perda ou de ser corrompida.	Em até 30 minutos
Gravidade 2: Um problema ocorreu, causando danos graves à uma funcionalidade importante. As operações do Cliente podem prosseguir de forma restrita, entretanto a produtividade poderá ser afetada em longo prazo.	Em até 2 horas
Gravidade 3: Um problema ocorreu, causando efeitos colaterais limitados às operações comerciais do Cliente.	Em até um dia útil**
Gravidade 4: Um problema ocorreu onde as operações comerciais do Cliente não foram afetadas negativamente.	Até o próximo dia útil. A Symantec recomenda que o Cliente envie sugestões sobre novos recursos ou aprimoramentos aos fóruns da Symantec

Os Objetivos de resposta do suporte acima são alcançáveis durante as operações normais de serviço e não são aplicados durante a Manutenção para o Serviço e/ou suporte de infraestrutura conforme descrito na seção de Manutenção abaixo.

** Os objetivos de tempos de resposta são referentes ao tempo de resposta à solicitação, e não ao tempo de resolução (o tempo que leva para fechar a solicitação).*

*** Um "dia útil" significa as horas úteis regionais padrão e os dias da semana no fuso horário local do Cliente, excluindo fins de semana e feriados públicos locais. Na maioria dos casos, "horas úteis" significam das 9h às 17h no fuso horário local do Cliente.*

Manutenção para o Serviço e/ou suporte de Infraestrutura de Serviço

A Symantec deve executar manutenções regulares. A Symantec fará esforços comercialmente razoáveis para fazer manutenção de rotina quando houver baixa atividade coletiva do Cliente para minimizar a interrupção. O Cliente não receberá notificação prévia para essas atividades de manutenção de rotina. Para outros tipos de manutenção e como listado abaixo, a Symantec fará esforços para informar as partes afetadas com antecedência por meio da publicação de um alerta na página de status da Symantec (https://status.symantec.com/). Para ver informações sobre status do Serviço, manutenções planejadas e problemas conhecidos, acesse a Página de status da Symantec e cadastre-se na página Symantec Email Security.cloud para receber as últimas atualizações. **Recursos principais do Serviço, como Verificação de segurança e Entrega de email, não são interrompidos durante todas as atividades de manutenção.**

- ***Manutenção Planejada:*** Manutenções planejadas são os períodos de manutenção agendados, durante os quais o Serviço pode ser interrompido ou impedido devido à indisponibilidade da Infraestrutura do Serviço. A Symantec fará esforços para executar a Manutenção planejada quando houver baixa atividade coletiva do Cliente, no fuso horário em que a Infraestrutura estiver localizada e somente em uma parte da rede (e não em toda a rede). Durante a Manutenção planejada, o Serviço poderá ser direcionado para seções da Infraestrutura que não estiverem incluídas na manutenção, e, por isso, o Serviço poderá não ser interrompido. Para a Manutenção planejada, a Symantec fará todo o esforço comercialmente razoável para publicar uma notificação para o Cliente na Página de status da Symantec, com sete (7) dias corridos de antecedência. Para receber notificações por SMS, email ou pelo Twitter, os Clientes podem se cadastrar na Página de status da Symantec.

- ***Manutenção Não Planejada:*** Manutenções não planejadas são períodos de manutenção planejada que não permitem a notificação padrão de sete (7) dias e durante os quais o Serviço pode ser interrompido ou impedido devido à indisponibilidade da Infraestrutura do Serviço. A Symantec fará esforços comercialmente razoáveis para enviar ao Cliente uma notificação de no mínimo um (1) dia publicada na Página de status da Symantec. Durante a Manutenção não planejada, o Serviço poderá ser direcionado para seções da Infraestrutura que não estiverem incluídas na manutenção, e, por isso, o Serviço poderá não ser interrompido. Em certos momentos, a Symantec fará a Manutenção de Emergência. A Manutenção de Emergência é a manutenção que *deve ser implementada o mais rápido possível para resolver ou impedir um incidente maior*. A Symantec fará todos os esforços para informar as partes afetadas com antecedência por meio da publicação de um alerta na Página de status da Symantec em até uma (1) hora antes do início da manutenção.
- ***Manutenção do Console de Gerenciamento:*** Para Manutenção do console de gerenciamento, a Symantec fará todo o esforço comercialmente razoável para publicar uma notificação para o Cliente na Página de status da Symantec, com quatorze (14) dias corridos de antecedência. A Symantec fará todos os esforços para executar a manutenção no Console de gerenciamento quando houver baixa atividade coletiva do Cliente, a fim de minimizar a interrupção da disponibilidade do console. Em determinadas ocasiões, a Symantec pode fazer pequenas atualizações no Console de gerenciamento, mas o Cliente não receberá notificação prévia para essas atividades de manutenção de rotina.

5: Termos adicionais

- O Serviço pode ser acessado e usado em todo o mundo, conforme as limitações de conformidade de exportação e limitações técnicas de acordo com os padrões atuais da Symantec.
- A Symantec reserva-se o direito de modificar e atualizar os recursos e a funcionalidade do Serviço com o objetivo de fornecer um Serviço igual ou melhor (desde que a Symantec não reduza materialmente a funcionalidade principal do Serviço). O Cliente reconhece e concorda que a Symantec reserva-se o direito de atualizar esta Descrição de Serviço a qualquer momento durante o Prazo da Assinatura para refletir com precisão o Serviço sendo prestado, e a Descrição de Serviço atualizada entrará em vigor no momento que for publicada.
- O uso de todos os Componentes do Serviço, na forma de software, deverá ser regido pelo contrato de licença que acompanha o software. Se nenhum EULA acompanhar o Componente do Serviço, ele deverá ser regido pelos termos e condições localizados em (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Todos os outros direitos e obrigações relacionados ao uso do Componente do Serviço deverão ser estabelecidos conforme esta Descrição de Serviço.
- Exceto conforme especificado na Descrição de Serviço, o Serviço (incluindo qualquer componente do Software do Serviço hospedado aqui fornecido) poderá usar código-fonte aberto e materiais de terceiros que estão sujeitos a uma licença separada.
- A Symantec poderá atualizar o Serviço a qualquer momento a fim de manter a eficácia do Serviço.
- Todos os modelos fornecidos pela Symantec são destinados a uso exclusivo como guia para que o Cliente aprenda a criar suas próprias políticas personalizadas, bem como outros modelos.
- Os limites abaixo se aplicam ao Serviço:
    - Mensagens de entrada e de saída, por usuário, por mês = dez mil (10.000) Esse limite não inclui spam e malware direcionados ao Cliente.
    - A Symantec se reserva o direito de enviar uma fatura ao Cliente pelos usuários adicionais, após notificação, pelos meses restantes do contrato de Serviço, quando o uso exceder o limite de mensagens.
    - Agendamento de novas tentativas de envio e recebimento de emails = sete (7) dias consecutivos.
    - Tamanho de email máximo padrão = cinquenta megabytes (50 MB). O Cliente pode especificar um tamanho máximo qualquer de Email em até um mil megabytes (1000 megabytes). Os Emails recebidos pelo Serviço que excederem o limite especificado serão bloqueados e excluídos, e um Email de alerta de notificação será enviado ao remetente, ao destinatário pretendido e a um Administrador.
    - Rastreamento de mensagens = os dados ficam disponíveis para pesquisas de soluções de problemas por 30 dias; limites adicionais se aplicam a uma quantidade de resultados que podem ser retornados por uma única pesquisa.
    - Quarentena de malware = Emails são automaticamente excluídos após trinta (30) dias.
    - Quarentena de spam = Emails são automaticamente excluídos após catorze (14) dias, exceto se for configurado de outra forma.
    - Disponibilidade de dados do relatório do painel = quarenta (40) dias para informações detalhadas; doze (12) meses para informações de resumo.
    - Disponibilidade de dados do relatório de resumo (PDF) = doze (12) meses.
    - Disponibilidade de dados do relatório detalhado (CSV) = quarenta (40) dias.

- As limitações abaixo se aplicam ao Policy Based Encryption:
  - Emails de saída (Z) com o Policy Based Encryption por usuário, por mês = trezentos (300)
  - Emails de saída do Policy Based Encryption Essentials/Advanced por usuário, por mês = quatrocentos e oitenta (480).
  - Quando o envio é feito a vários destinatários, cada endereço exclusivo é considerado como um Email seguro. Caso o Cliente exceda o número de Emails seguros permitidos em um mês, a Symantec se reserva o direito de enviar uma fatura ao Cliente pelo uso real.
  - Os Emails direcionados pelo Policy Based Encryption Service estão limitados a um tamanho máximo de cinquenta megabytes (50 MB).
  - Se a criptografia Pull estiver sendo usada com Policy Based Encryption Service (Z) por padrão, os Emails serão armazenados por 90 dias no portal de coleta seguro, antes da expiração.
  - Se a criptografia Pull estiver sendo usada com o Policy Based Encryption Advanced Service por padrão, os Emails serão armazenados por 30 dias no portal de coleta seguro, antes da expiração.
  - Os níveis de serviço de Disponibilidade e Latência não se aplicam a este Serviço.

- Para garantir que as mensagens permaneçam seguras durante toda a transmissão, a Symantec recomenda que o Cliente configure os domínios que serão usados para o Policy Based Encryption, de forma que a criptografia TLS seja imposta em todas as mensagens de entrada e de saída através da Infraestrutura do Serviço.
- Os Clientes deverão direcionar os Emails de entrada através da Symantec, usando as informações de roteamento fornecidas pela Symantec, e não deverão direcionar Emails a uma Torre ou a um endereço IP específico.
- O Serviço só está disponível a um Cliente que tenha seu próprio nome de domínio de Email e que tenha a capacidade de configurar os registros MX e/ou DNS para esse nome de domínio.
- O Cliente deverá aceitar Emails de entrada de todas as faixas de IP exigidas, a fim de garantir a continuidade do serviço, caso uma parte da Infraestrutura não esteja disponível.
- O Cliente deverá especificar os endereços IP do servidor de email ou o nome dos hosts para a entrega de Emails de saída à sua empresa.
- O Cliente deverá verificar se todos os domínios (incluindo os subdomínios) que exigem o Serviço são provisionados. O Cliente aceita que os recursos do Serviço podem não funcionar corretamente e que a entrega do Email poderá não estar disponível para os domínios que não forem provisionados. O Cliente concorda em fornecer e manter uma lista de endereços de Email válidos para receber o Serviço (a "Lista de Validação"). É responsabilidade do Cliente verificar a Lista de Validação antes que o Serviço seja disponibilizado e no período de duração do Serviço. Emails que forem enviados a endereços não contidos na Lista de Validação, ou que forem inseridos incorretamente, serão rejeitados pelo Serviço. O Cliente aceita que os SLAs não se aplicarão a Emails enviados a endereços inválidos. Para evitar dúvidas, os Clientes que estiverem usando o sistema de Quarentena de spam deverão manter uma Lista de Validação e ativar o recurso Registro de Endereços. Se o Cliente não puder fornecer essa Lista de Validação e exigir que o recurso de Registro de endereços seja desativado, a Symantec analisará cada solicitação individualmente e se reservará o direito de recusar solicitações, a critério único e absoluto da Symantec.
- O Cliente poderá liberar os Emails que tiverem sido categorizados como portadores de malware ou spam, ou solicitar que a Symantec libere esses Emails no domínio do Cliente. O CLIENTE CONCORDA QUE A SYMANTEC NÃO PODERÁ ACEITAR NENHUMA RESPONSABILIDADE PELA LIBERAÇÃO DE TAIS EMAILS, MEDIANTE A SOLICITAÇÃO DO CLIENTE.
- A Symantec não se responsabiliza por nenhum dano ou perda resultante direta ou indiretamente de alguma falha do Serviço na identificação de spam, ou por identificar incorretamente um Email como portador de malware ou spam. A Symantec se reserva o direito de verificar todos os Emails de saída.
- Uma mensagem padrão de isenção de responsabilidade será aplicada aos Emails que forem verificados pelo Serviço a partir do início do provisionamento deste. O texto da mensagem será editado pelo Cliente por meio do console de gerenciamento. A Symantec se reserva o direito de atualizar a mensagem padrão de isenção de responsabilidade a qualquer momento.
- O Cliente deve estar em conformidade com todas as leis aplicáveis com relação ao uso do Serviço. Em determinados países, poderá ser necessário obter o consentimento de funcionários específicos. O Cliente tem poder total de configuração e o uso do Serviço; portanto, a Symantec não será responsabilizada pelo uso que o Cliente fizer do Serviço, nem responsabilizada por qualquer responsabilidade civil ou criminal incorrida pelo Cliente como consequência da operação do Serviço.
- Caso o provisionamento contínuo do Serviço ao Cliente comprometa a segurança do Serviço, incluindo, entre outros, tentativas de atividades de hackers, ataques de negação de serviço, carta bomba ou outras atividades maliciosas direcionadas ou originadas dos domínios

do Cliente, o Cliente concorda que a Symantec poderá suspender temporariamente o Serviço ao Cliente. Nesse caso, a Symantec informará o Cliente imediatamente e trabalhará com ele para resolver os problemas. A Symantec restabelecerá o Serviço após a remoção da ameaça à segurança.

- Caso um Serviço seja suspenso por qualquer motivo, ele não será aplicado aos Emails do Cliente, e os Emails não serão direcionados através da Infraestrutura da Symantec. O Cliente é responsável pelo redirecionamento de seus Emails durante a suspensão e pela confirmação de que todas as configurações estão precisas, caso o Serviço seja restabelecido.
- Caso o Serviço seja encerrado por qualquer motivo, a conta do Cliente será excluída e o Cliente não terá acesso ao Serviço.
- O Cliente não deverá permitir que seus sistemas: (i) atuem como Retransmissão Aberta ou Proxy Aberto; ou (ii) enviem spam. A Symantec se reserva o direito de analisar a conformidade do Cliente com esta seção a qualquer momento. Para evitar dúvidas, qualquer violação desta Cláusula constituirá uma violação material do Contrato, e a Symantec se reserva o direito de suspender todo o Serviço ou parte dele imediatamente até que a violação seja corrigida, ou encerrar o Contrato relacionado ao Serviço afetado.
- Se em algum momento (i) os sistemas de Email do Cliente forem incluídos em blacklists ou (ii) o Cliente for responsável pela inclusão dos sistemas da Symantec em blacklists devido ao envio de spam, ou (iii) o Cliente não cumprir com as obrigações definidas nesta Descrição de Serviço, a Symantec informará o Cliente e se reservará o direito, a seu próprio critério, de suspender, interromper ou encerrar todo o Serviço ou parte dele.
- O Cliente tem permissão de usar o Serviço somente para seus próprios fins comerciais. O Cliente concorda em não revender, sublicenciar, fazer leasing de, ou de alguma outra forma disponibilizar o Serviço e a documentação associada a terceiros. O Cliente concorda em não usar o Serviço para fins de criação de um produto ou serviço concorrente ou copiar seus recursos ou interface do usuário, executar avaliações, testes de desempenho ou análises comparativas do Serviço para fins de publicação fora da empresa do Cliente, sem o consentimento prévio, por escrito, da Symantec.

6: Definições

"**Registro de Endereços**" é um recurso compulsório do Serviço que rejeita Emails de entrada que foram enviados a endereços de Email não incluídos na lista de endereços de Email válidos do Cliente (a "Lista de Validação").

"**Administrador**" significa um Usuário do Cliente com autorização para gerenciar o Serviço em nome do Cliente. Os administradores poderão gerenciar todo o Serviço ou parte dele, conforme designado pelo Cliente.

"**Configurações das Melhores Práticas de AntiSpam**" são as diretrizes de configuração recomendadas pela Symantec para o Serviço, conforme fornecidas ao Cliente durante o processo de provisionamento ou conforme publicado no recurso de ajuda online.

"**Gerenciador de Conexões**" são os métodos de detecção estabelecidos no estágio de aperto de mão do SMTP.

"**Solicitação de Crédito**" é a notificação que o Cliente deve enviar à Symantec por email para support.cloud@symantec.com com a linha de assunto "Solicitação de Crédito" (a menos que notificado de outra forma pela Symantec).

"**Cluster de Torres Designadas**" são duas (2) ou mais Torres designadas para fornecer o Email Security Services ao Cliente.

"**Configurações do Nível do Domínio**" são configurações de domínio que são personalizáveis para um determinado domínio no console de gerenciamento para os Email Security Services.

"**Email**" são todas as mensagens SMTP de entrada e de saída que passam pelo Serviço.

"**Email Security Services**" são as opções Email Safeguard e Email Protect e todos os serviços complementares disponíveis.

"**Falsos Positivos de Malware em Email**" são Emails legítimos identificados incorretamente como portadores de malware.

"**Contrato de Licença do Usuário Final (EULA)**" são os termos e condições que acompanham o Software (conforme definido abaixo).

"**Configurações Globais**" são as ações no console de gerenciamento que são aplicadas a todos os domínios e níveis de grupo para os Serviços.

"**Configurações de Nível de Grupo**" são configurações de grupo que são personalizáveis para um determinado grupo no console de gerenciamento para os recursos aplicáveis do Serviço.

"**Infraestrutura**" significa qualquer tecnologia do licenciador ou da Symantec e a propriedade intelectual usada para fornecer os Serviços.

"**Malware Conhecido**" é um malware para o qual, no momento do recebimento do conteúdo pela Symantec, uma assinatura já tenha sido disponibilizada por no mínimo uma (1) hora, para uso pelas tecnologias de antivírus implementadas pela Symantec.

"**Malware**" ou "**software malicioso**" é qualquer software usado para interferir nas operações de computadores ou dispositivos móveis, ou sem autorização apropriada, usado para coletar informações confidenciais e/ou para obter acesso a sistemas de computadores privados.

"**Falsos Positivos de Malware**" são Emails legítimos identificados incorretamente como portadores de malware.

"**Membro**" é o Cliente e terceiros com os quais o Cliente cria uma rede criptografada, utilizando o Serviço complementar Email Boundary Encryption legado.

"**Cobrança Mensal**" é cobrança mensal do Serviço afetado, conforme definido no Contrato.

"**Ajuda Online** " são as informações adicionais disponíveis em http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=PT_BR.

"**Proxy Aberto**" é um servidor proxy configurado para permitir que pessoas desconhecidas ou não autorizadas acessem, armazenem ou encaminhem DNS, páginas da Web ou outros dados para o Serviço.

"**Retransmissão Aberta**" é um servidor de Email configurado para receber Emails de pessoas desconhecidas ou não autorizadas e encaminhar os Emails a um ou mais destinatários que não sejam usuários do sistema de Email ao qual o servidor de Email está conectado. Retransmissão Aberta pode também ser chamada de "Retransmissão de Spam" ou "Retransmissão Pública".

"**Confirmação do Pedido**" tem o seu significado determinado nos Termos e Condições dos Serviços online da Symantec, caso aplicáveis. Caso não haja Termos e condições aplicáveis ao Serviço, a "Confirmação do Pedido" será o Instrumento de Assinatura, conforme aqui definido.

"**Serviço**" é a opção Protect ou Safeguard do Symantec Email Security.cloud, adquirida pelo Cliente.

"**Componente do Serviço**" refere-se a certos softwares de capacitação, periféricos de hardware e documentação associada, que podem ser fornecidos separadamente pela Symantec como parte incidental de um Serviço.

"**Crédito de Serviço**" é a quantia monetária que será creditada na próxima fatura do Cliente após o envio de uma Solicitação de Crédito e validação pela Symantec de que o crédito deve ser pago ao Cliente.

"**Software do Serviço**" significa o Software (definido abaixo), conforme poderá ser requisitado por um Serviço, e que deverá ser instalado em cada computador do Cliente, para que possa receber o Serviço. O Software do Serviço inclui o Software e a documentação associada, que podem ser fornecidos separadamente pela Symantec, como parte do Serviço.

"**Software**" refere-se a cada programa de software da Symantec ou do licenciador, em formato de código do objeto, licenciado ao Cliente pela Symantec e regido pelos termos do EULA correspondente, incluindo, sem limitações, novas versões ou atualizações, conforme aqui fornecido.

"**Spam**" refere-se a Emails comerciais não solicitados.

"**Falso Negativo de Spam**" refere-se a Emails de spam que não são identificados como spam pelo Serviço.

"**Falso Positivo de Spam**" refere-se a Emails identificados incorretamente como Spam pelo Serviço.

"**Configurações Recomendadas para Spam**" são as diretrizes de configuração recomendadas pela Symantec para o Serviço, conforme fornecidas ao Cliente durante o processo de provisionamento ou conforme publicadas no recurso de ajuda online.

"**Instrumento de Assinatura**" significa um ou mais dos documentos aplicáveis, que define ainda mais os direitos e as obrigações relacionados ao Serviço: um certificado da Symantec ou documento semelhante emitido pela Symantec ou um contrato por escrito entre o Cliente e a Symantec, que acompanha, precede ou segue o Serviço.

"**Termos do Symantec Hosted Services**" são os Termos dos Symantec Hosted Services, localizados ou acessados via https://www.symantec.com/about/legal/service-agreements.jsp.

"**Termos e Condições dos Serviços Online da Symantec**" são os Termos e Condições dos Serviços Online localizados ou acessados em https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Tracker**" é uma ferramenta da Symantec através da qual a Disponibilidade e Latência de Serviço são avaliadas para o Serviço.

"**Torre**" é um cluster de servidores de Email para balanceamento de carga.

"**Usuário**" é um indivíduo que envia e recebe emails e está protegida por qualquer parte do Serviço.

Anexo A

Contrato de Nível de Serviço

Geral

- O Cliente poderá ter direito a um Crédito de Serviço se a Symantec não cumprir o nível do serviço definido. Se o Cliente acreditar que tem direito a um Crédito de Serviço, ele deverá enviar uma Solicitação de Crédito dentro de dez (10) dias úteis antes do último dia do mês no qual a suspeita falha na conformidade do nível do serviço tiver ocorrido. O Cliente reconhece que os logs são mantidos somente por um período de tempo limitado e, portanto, solicitações de Crédito enviadas fora do prazo determinado serão consideradas inválidas.
- Uma Solicitação de Crédito deverá ser feita através do Suporte Técnico da Symantec. Acesse a página inicial do suporte ao produto para obter instruções detalhadas encontradas em: https://support.symantec.com/en_US/email-security-cloud..html.
- Todas as Solicitações de Crédito estarão sujeitas à verificação da Symantec de acordo com as provisões aplicáveis deste Contrato de Nível de Serviço. A Symantec poderá solicitar mais informações do Cliente para validar a Solicitação de Crédito.
- Este Contrato de Nível de Serviço não estará operante: (i) durante períodos de Manutenção Planejada ou Manutenção de Emergência, períodos de não disponibilidade devido a motivos de força maior e atos ou omissões por parte do Cliente ou de terceiros; (ii) durante qualquer período de suspensão do serviço pela Symantec, de acordo com os termos do Contrato; (iii) quando o Cliente violar o Contrato (incluindo, sem limitações, quando o Cliente tiver faturas pendentes); (iv) quando o Cliente não tiver configurado o Serviço de acordo com o Contrato; ou (v) durante períodos do serviço de teste.
- As correções definidas neste Contrato de Nível de Serviço serão correções únicas e exclusivas do Cliente em contrato, delito (incluindo, sem limitações, negligências) ou de outra forma, em relação a este Contrato de Nível de Serviço.
- A responsabilidade máxima acumulada da Symantec de acordo com este Contrato de Nível de Serviço em qualquer mês será um crédito igual ou inferior a 100% da Cobrança Mensal ou dez mil dólares/cinco mil libras esterlinas/dez mil euros (US$ 10.000/£ 5.000/€ 10.000) (dependendo da moeda da fatura recebida pelo Cliente).
- Se o Serviço afetado for adquirido como parte de um pacote de Serviços, o Crédito de Serviço será calculado com base no Serviço afetado e não no pacote inteiro de Serviços.

Exceções do Contrato de Nível de Serviço para o Email Security Services

Este Contrato de Nível de Serviço não estará operante: (i) em relação aos Emails que não passarem pelo Serviço (incluindo, sem limitações, se o Cliente não tiver tomado as medidas apropriadas para garantir que só aceitará Emails de entrada da infraestrutura da Symantec); (ii) em relação aos Emails de entrada e de saída que tenham sido inicialmente enviados à Symantec, e que contenham mais de 500 destinatários por sessão de SMTP, (iii) para os clientes provisionados em uma Torre designada como Torre de cluster em massa, ou (iv) em relação aos Emails de entrada e saída pelos domínios do Cliente, que não tiverem sido provisionados para o Serviço.

Disponibilidade do Serviço

O Nível de Serviço da Disponibilidade do Serviço é definido pela habilidade de estabelecer uma sessão de SMTP na porta 25 do MTA do Cliente para a Infraestrutura da Symantec, em conformidade com o RFC5321. O Nível de Serviço da Disponibilidade do Serviço não se aplica ao portal de gerenciamento ou ao sistema de quarentena de spam. Esse nível de serviço não será aplicado se o Cliente tiver configurado incorretamente o Serviço devido a circunstâncias imprevisíveis ou causas fora do controle razoável da Symantec, incluindo, sem limitações, desastres naturais, guerras, atos de terrorismo, motins, ações governamentais ou uma falha na rede ou em dispositivos fora dos data centers da Symantec, incluindo em sites do Cliente ou entre o site do Cliente e o datacenter da Symantec.

Se a Disponibilidade do Serviço for inferior a cem por cento (100%) em um mês, o Cliente poderá enviar uma solicitação de crédito e poderá receber um Crédito de Serviço para o crédito da porcentagem seguinte, igual ou inferior a 100% da cobrança mensal ou dez mil dólares/cinco mil libras esterlinas/dez mil euros (US$ 10.000/£ 5.000/€ 10.000) (dependendo da moeda da fatura recebida pelo Cliente):

Porcentagem disponível por mês do calendário	Porcentagem de crédito da cobrança mensal
abaixo de 100% e acima ou igual a 99%	25%

abaixo de 99% e acima ou igual a 98%	50%
abaixo de 98%	100%

Se a Disponibilidade do Serviço for inferior a noventa e oito por cento (98%) em qualquer mês, confirmado pela Symantec, o Cliente terá direito a encerrar o Serviço afetado e receber um reembolso proporcional ou as tarifas pagas antecipadamente para a porção do período após a efetivação de tal encerramento.

Entrega de email

O nível do Serviço de Entrega de Emails é definido pela habilidade da Symantec de entregar 100% de todos os Emails enviados pelo Cliente ou para o Cliente, sujeito às seguintes condições:

a) O Email deverá ter sido recebido pela Symantec e

b) O Email não deverá conter um malware, spam ou outro conteúdo que possa causar a sua interceptação pelo Serviço.

Sujeito às condições acima, caso a Symantec não consiga entregar um Email enviado ou recebido pelo Cliente, o Cliente não estará violando os termos do Contrato. O Cliente tem o direito a encerrar o Serviço dentro de trinta (30) dias corridos, após aviso por escrito.

Latência do email

O Nível do Serviço de Latência do Email é definido pelo tempo médio de retorno, em um mês corrido, conforme medido pelo Symantec Tracker, de Emails enviados a cada cinco (5) minutos entre todas as torres do Cluster de Torres Designadas do Cliente, avaliando se esse tempo excede os atrasos determinados na tabela abaixo. Se o Cliente acreditar que o Nível do Serviço de Latência não foi cumprido, ele poderá enviar uma Solicitação de Crédito e receber um Crédito de Serviço, de acordo com a tabela abaixo:

Tempo de retorno médio (em segundos)	Porcentagem de crédito da cobrança mensal
acima de 60 e abaixo ou igual a 90	25%
acima de 90 e abaixo ou igual a 120	50%
acima de 120 e abaixo ou igual a 180	75%
acima de 180	100%

Esse Nível de Serviço de Latência não será aplicável se:

a) O Cliente não tiver fornecido à Symantec a Lista de Validação e o Cliente sofrer um ataque de negação de serviço;

b) Os períodos de atraso forem causados por um loop de emails enviados ou recebidos pelos sistemas do Cliente;

c) O principal servidor de Email do Cliente não puder aceitar Emails na primeira tentativa de entrega.

Falsos positivos de spam

O Nível do Serviço de Falsos Positivos de Spam define a taxa máxima de captura de falsos positivos de spam. O Nível do Serviço de Falsos Positivos de Spam se aplicará somente se o Cliente implementar as Configurações de Melhores Práticas de AntiSpam, conforme determinado no recurso Ajuda Online. Se a taxa de captura média dos Falsos Positivos de Spam ficar acima de 0,0003% do tráfego de entrada de Emails do Cliente em um mês corrido, o Cliente poderá enviar uma Solicitação de Crédito e poderá receber um Crédito de Serviço, de acordo com a tabela abaixo:

Taxa % de captura de falsos positivos de spam	Porcentagem de crédito da cobrança mensal
acima de 0,0003 e abaixo ou igual a 0,003	25%

acima de 0,003 e abaixo ou igual a 0,03	50%
acima de 0,03 e abaixo ou igual a 0,3	75%
acima de 0,3	100%

Os Emails abaixo não constituem falsos positivos de spam para os fins deste nível de serviço:
a) Emails que não forem Emails comerciais legítimos;
b) Emails com mais de 20 destinatários;
c) Emails cujo remetente estiver na lista de remetentes bloqueados do Cliente, incluindo, sem limitações, aqueles definidos pelo usuário individual, se o Cliente tiver ativado as configurações no nível de usuário;
d) Emails enviados de um computador comprometido;
e) Emails enviados de um computador que estiver na lista de bloqueios de terceiros;
f) Emails interceptados pela verificação de spam de saída.

Para ter direito a um Crédito de Serviço, o Cliente deverá relatar Emails de falsos positivos suspeitos ao Suporte Técnico da Symantec até cinco (5) dias corridos após o recebimento do Email. A Symantec investigará e confirmará se o Email é ou não um falso positivo de spam e registrará o resultado.

Taxa de captura de spam
O Nível de Serviço da Taxa da Captura de Spam define a taxa mínima de captura de spam. O nível de serviço será aplicado somente se o Cliente implementar as Configurações de Melhores Práticas de AntiSpam, conforme determinado no recurso Ajuda Online. O nível de serviço corresponde à quantidade de falsos negativos de spam detectados em um mês. O Cliente poderá enviar uma Solicitação de Crédito e receber um Crédito de Serviço de acordo com a tabela abaixo:

Taxa de % de captura de spam	Porcentagem de crédito da cobrança mensal
acima de 98 e abaixo ou igual a 99	25%
acima de 97 e abaixo ou igual a 98	50%
acima de 96 e abaixo ou igual a 97	75%
abaixo de 96	100%

O Nível de Serviço da Taxa de Captura de Spam não será aplicável se o Email não tiver sido enviado a um endereço de Email válido. Uma taxa de captura de spam mais baixa de noventa e cinco por cento (95%) será aplicada a Emails que contiverem mais de cinquenta por cento (50%) dos conjuntos de caracteres de dois bytes. Caso a taxa de captura de spam seja inferior a noventa e cinco por cento (95%), o Cliente terá direito a um Crédito de Serviço de vinte e cinco por cento (25%) da cobrança mensal. Caso a taxa de captura de spam seja inferior a noventa por cento (90%), o Cliente terá direito a um Crédito de Serviço equivalente a cem por cento (100%) da cobrança mensal.

Para ter direito a um Crédito de Serviço, o Cliente deverá relatar Emails de falsos negativos suspeitos ao Suporte Técnico da Symantec até cinco (5) dias corridos após o recebimento do Email. A Symantec investigará e confirmará se o Email é ou não um falso negativo de spam e registrará o resultado.

Proteção contra malware
Se os sistemas do Cliente estiverem infectados por malware conhecido ou desconhecido que se propaga através de Emails que passam pelo serviço de verificação na nuvem, o Cliente poderá ter direito a um Crédito de Serviço, no valor definido abaixo. O Cliente deverá notificar a Symantec dentro

de cinco (5) dias após o descobrimento do malware, e tal notificação deverá ser registrada em log, investigada e validada pela Symantec. O Cliente deverá enviar uma Solicitação de Crédito e, se validada, poderá receber um Crédito de Serviço igual ou inferior a cem por cento (100%) da cobrança mensal ou dez mil dólares/cinco mil libras esterlinas/dez mil euros (US$ 10.000/£ 5.000/€ 10.000) (dependendo da moeda da fatura recebida pelo Cliente). A correção definida nesta seção deverá ser a correção única e exclusiva em contrato, delito (incluindo, sem limitações, negligências) ou outra forma em relação a qualquer infecção por malware transmitida ao Cliente ou a terceiros por meio do Serviço. Para evitar dúvidas, a correção definida nesta seção não se aplicará em casos de autoinfecção proposital.

Os sistemas do Cliente são considerados infectados se um malware anexado a um Email for recebido por meio do Serviço e o malware tiver sido ativado no sistema do Cliente, automaticamente ou com intervenção manual. Caso a Symantec detecte, mas não bloqueie um Email que contenha um malware anexado, e publique uma atualização na página de status da Symantec ou de outra forma notifique os Clientes, fornecendo informações suficientes para que o Cliente identifique e exclua o Email infectado, a correção acima não será aplicável.

O Serviço fará a mais abrangente verificação possível do Email e de seus anexos. Talvez não seja possível realizar a verificação em anexos com conteúdo que esteja sob o controle direto do remetente (*por exemplo*, anexos protegidos por senhas e/ou criptografados e/ou senhas que são enviadas separadamente do Email). Esses Emails e/ou anexos são excluídos do nível de serviço, e a correção definida acima não é aplicada.

Esse Nível de Serviço de Proteção contra Malware não estará em operação para malware que tenha sido lançado propositalmente pelo Cliente ou pela Symantec segundo solicitação do Cliente.

Esse Nível de Serviço de Proteção contra Malware será aplicado somente a Malwares conforme definido nesta Descrição de Serviço e não se aplicará ao seguinte: spyware, adware, links de URL a sites que hospedam conteúdo malicioso ou cavalos de Troia desconhecidos.

Falsos positivos de malware

O Nível de Serviço de Falsos Positivos de Malware define a taxa máxima de captura de falsos positivos de malware. Se a taxa de captura média dos Falsos Positivos de Malware ficar acima de 0,0001% do tráfego de entrada de Emails do Cliente em um mês corrido, o Cliente poderá enviar uma Solicitação de Crédito e poderá receber um Crédito de Serviço, de acordo com a tabela abaixo:

Taxa % de captura de falsos positivos de malware	Porcentagem de crédito da cobrança mensal
acima de 0,0001 e abaixo ou igual a 0,001	25%
acima de 0,001 e abaixo ou igual a 0,01	50%
acima de 0,01 e abaixo ou igual a 0,1	75%
acima de 0,1	100%

Suporte técnico e resposta a falhas 24 horas por dia, 7 dias por semana

O Suporte Técnico está disponível vinte e quatro (24) horas por dia, sete (7) dias por semana para:

a) fornecer suporte técnico aos Clientes que encontrarem problemas com o Serviço e

b) comunicar-se com o Cliente para resolver tais problemas.