Gateway de conexão segura

Nossa tecnologia integra a proteção de dados e a prevenção contra ameaças em uma experiência de suporte automatizada e segura

Até

60%

dos líderes de TI que responderam à pesquisa pela Forrester aproveitam a tecnologia de conectividade para reduzir riscos[1]

Ela também é implementada como uma versão de conexão direta para o hardware Dell EMC selecionado e como um plug-in de Serviços no OpenManage Enterprise para servidores PowerEdge. A Dell Technologies Services está comprometida a implementar recursos de segurança, com base em mercados, normas e insights dos clientes, que ajudam nossos produtos a cumprir os objetivos de segurança e os requisitos de conformidade de nossos clientes.

Conteúdo

1: Introdução:

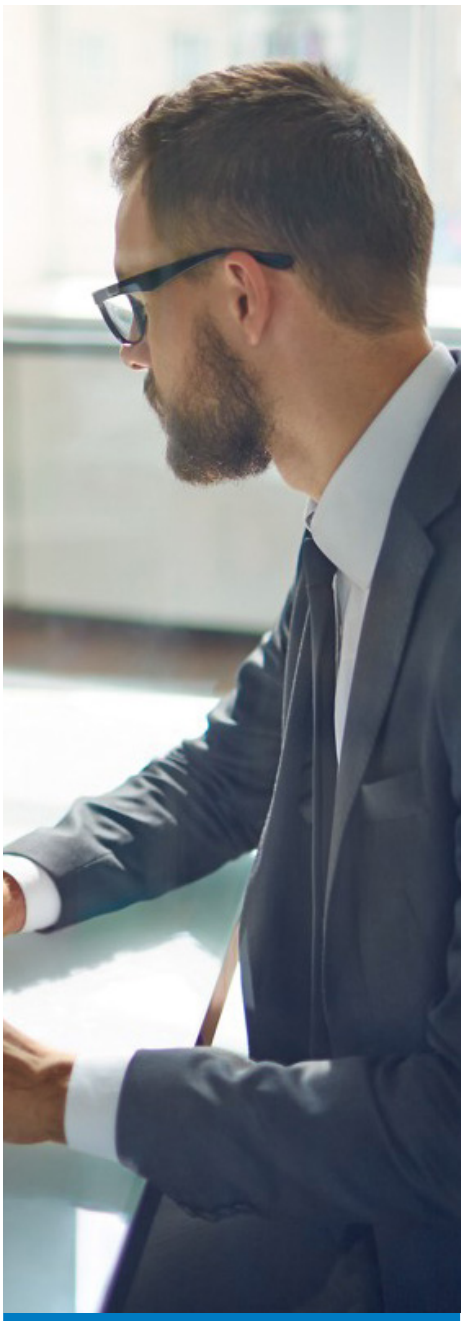
No mundo extremamente digital de hoje, os líderes em inovação bem-sucedidos buscam provedores de serviços de TI para terceirizar o suporte de TI. De acordo com um estudo da Forrester Consulting encomendado pela Dell Technologies Services[1], 59% dos líderes de TI afirmam que a parceria com o provedor de serviços de TI certo permite que as empresas transformem o tempo que a equipe de TI gasta com as operações diárias em iniciativas estratégicas e de inovação.

Como provedor líder de serviços de TI, a Dell Technologies Services tem o compromisso de garantir que seus serviços e tecnologias de suporte de TI não sejam fontes potenciais de ameaças à segurança. Todos os dias, fazemos tudo o que podemos para minimizar os riscos para os clientes com produtos Dell EMC implantados no ambiente deles. Este documento mostra como a segurança é integrada ao projeto, à implementação e à operação do gateway de conexão segura para garantir uma experiência automatizada e segura de suporte de TI em uma infraestrutura de data center complexa.

Valendo-se de mais de 25 anos de tecnologia pioneira em suporte de TI, a arquitetura de segurança do gateway de conexão segura foi projetada para evitar incursões de ameaças e proteger a integridade dos dados. Embora nossa tecnologia monitore continuamente os dispositivos dos clientes em busca de problemas e inicie a resolução acelerada:

- Utilizamos apenas dados de telemetria e eventos dos sistemas ativos.
- Criptografamos os dados de estado do sistema para transporte pela Internet por HTTPS usando o protocolo TLS.
- Nossos engenheiros de suporte técnico autorizados usam autenticação baseada em vários fatores para acessar e solucionar problemas remotamente em sistemas conectados.
- Processamos, armazenamos e usamos dados de telemetria e eventos em nossos locais usando as práticas de segurança líderes do setor.

Além disso, examinamos rigorosamente as medidas de segurança integradas em toda a arquitetura e nos processos do gateway de conexão segura com vários dos melhores fornecedores da categoria, como a Secureworks, para garantir que você tenha uma experiência confiável privada e segura.



Os ataques cibernéticos e a fraude ou o roubo de dados estão entre as cinco principais preocupações dos CEOs[2]

2: Sobre o Gateway de conexão segura

A Dell Technologies fornece tecnologia de conectividade segura que reduz as incertezas sobre a prevenção de problemas, permitindo que você tenha mais tempo para se concentrar nos projetos mais importantes. As versões de equipamento virtual e aplicativo fornecem uma conexão bidirecional segura entre seu ambiente e a Dell Technologies Services, o que é ideal para monitorar os dispositivos Dell EMC em seu data center, incluindo armazenamento de dados, servidores, sistema de rede, CI/HCI e proteção de dados, tudo em um único lugar.

Você também pode implementar nossa tecnologia com flexibilidade como uma versão de conexão direta para produtos Dell EMC selecionados e com um plug-in de Serviços no OpenManage Enterprise para servidores PowerEdge. Acesse Dell.com/Support para verificar as opções de conectividade compatíveis com hardware e software Dell EMC específicos.

Os dados são a base do gateway de conexão segura. Utilizamos os dados de estado do sistema obtidos dos ambientes do cliente. Eles são correlacionados com anos de dados de incidentes e de engenharia das equipes de suporte técnico e de campo, além de dados de fabricantes de componentes.

Consulte Itens reportáveis do Gateway de conexão segura e do plug-in de Serviços para OpenManage Enterprise para obter detalhes das informações de estado do sistema coletadas.

Usando modelos sofisticados de inteligência artificial, incluindo o aprendizado de máquina, nossa tecnologia de conectividade pode encontrar e aplicar padrões para detectar com precisão o problema que deve ser solucionado na primeira vez. Ela identifica problemas de hardware e software, cria um caso e inicia o contato conosco para começar a resolver uma situação antes que se torne um problema caro. Ela prevê falhas em discos rígidos de servidor e backplanes quando conectada por meio do gateway de conexão segura. Dependendo do tipo de problema, o alerta também pode iniciar uma remessa automática de peças.

Além disso, a tecnologia permite a comunicação bidirecional segura para que agentes de suporte técnico autorizados acessem remotamente dispositivos gerenciados para solucionar problemas e resolver questões.

SEGURANÇA PARA A CONECTIVIDADE

Avaliações de segurança de terceiros são feitas regularmente no gateway de conexão segura e em sua infraestrutura de suporte.

As avaliações de aplicativos incluem o transporte de dados e a segurança da API, a análise de código-fonte estático e dinâmico, as verificações cruzadas de CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e OWASP (Open Web Application Security Project, projeto de segurança de aplicativo da Web), além de bibliotecas e produtos de terceiros.

As **avaliações de infraestrutura** incluem dispositivos de rede internos e externos, servidores e provedores de serviços.

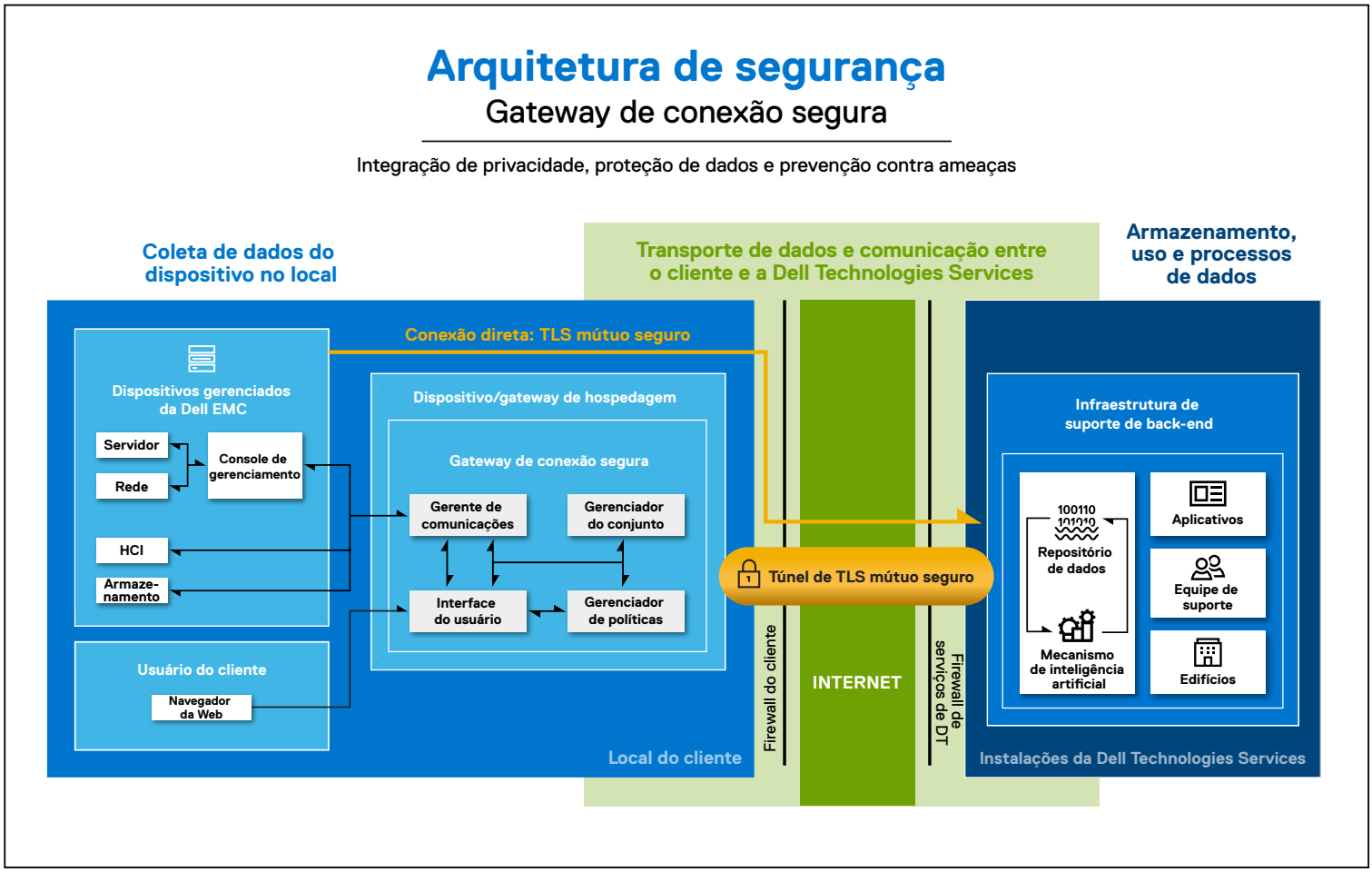
3: visão geral da arquitetura de segurança

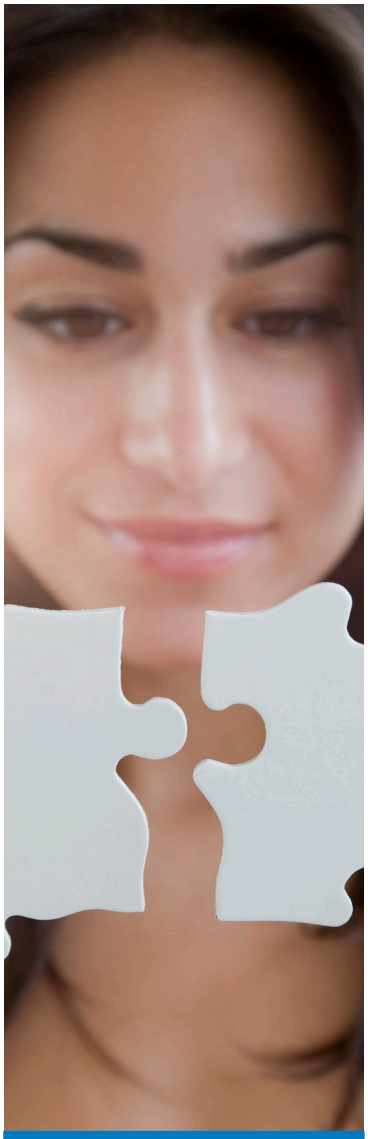
A Dell Technologies Services tem o compromisso de minimizar o risco de ameaças à segurança em nossa tecnologia de conectividade automatizada, proativa e preditiva. Nossa arquitetura de segurança foi desenvolvida de acordo com rigorosos padrões do setor e adota práticas de segurança mensuráveis e que podem ser repetidas em todas as etapas do desenvolvimento e da implementação do produto. Consulte a Seção 4 para obter mais informações.

O Diagrama A abaixo traz uma visão geral da arquitetura de segurança do gateway de conexão segura. Nas próximas seções, veremos como a nossa tecnologia coleta apenas os dados do sistema dos dispositivos gerenciados da Dell EMC necessários para diagnosticar e corrigir problemas e, depois, como ela processa esses dados do modo mais seguro e privado em:

- Coleta de dados do dispositivo no local
- Comunicação e transporte de dados
- Armazenamento de dados, uso e processos na Dell Technologies Services

Diagrama A:





Os clientes têm uma camada a mais de segurança para a coleta de dados no local por meio dos recursos de auditoria do gerenciador de políticas no gateway de conexão segura

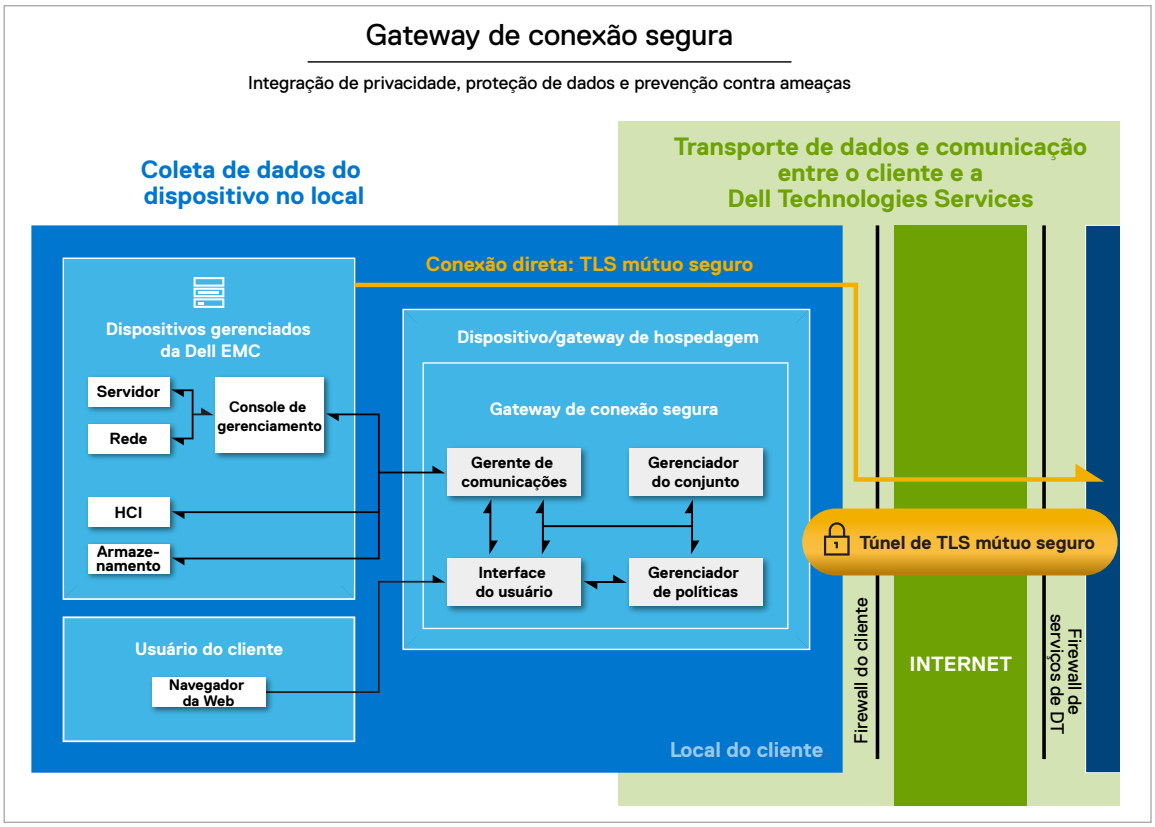
4: Abordagem detalhada para a segurança do Gateway de conexão segura

4-1: coleta de dados segura no local

Minimização dos pontos de acesso do firewall

O gateway de conexão segura agrega comunicações de todos os dispositivos da Dell EMC e atua como um ponto único de entrada e saída no firewall de um cliente para todas as atividades de serviços remotos com base em IP. Consulte o Diagrama B. Ao minimizar os pontos de acesso do firewall para a tecnologia de suporte remoto de TI, a Dell Technologies reduz o risco de segurança por meio do firewall da empresa.

Diagrama B: (trecho do diagrama A – Arquitetura de segurança):



Como um gateway no local, o gateway de conexão segura é implementado virtualmente em um hypervisor fornecido pelo cliente. Cada servidor de gateway age como um proxy, transferindo informações entre os dispositivos gerenciados. O gateway de conexão segura também pode criar uma fila de eventos de conexão no caso de uma falha temporária da rede local. Esses servidores de gateway têm sua própria interface de usuário da Web baseada no sistema operacional subjacente.

Para alguns clientes, a versão de conexão direta é adequada para a implementação heterogênea de vários produtos de hardware da Dell EMC. Essa solução funciona como um ponto único de comunicação seguro por meio do firewall do cliente. Ela é integrada ao ambiente operacional do produto e, portanto, não exige um servidor separado para fornecer suporte remoto de entrada e funcionalidade de call home.

Minimização dos pontos de acesso do firewall (continuação)

Para clientes em um data center com o PowerEdge que usam o console de gerenciamento de sistemas OpenManage Enterprise, o plug-in de Serviços incorporado é uma opção alternativa de implementação. Esse plug-in de conectividade no equipamento virtual do OpenManage Enterprise é executado em um hypervisor fornecido pelo cliente. Ele atua como uma camada de automação de serviços do servidor gerenciado e de dispositivos de chassi e fornece conexão direta única e segura com o back-end da Dell Technologies Services.

Atuação como um agente de comunicação seguro

O gateway de conexão segura funciona como agente de comunicação entre os dispositivos gerenciados, o gerenciador de políticas e a infraestrutura de suporte do back-end da Dell Technologies Services. Os servidores de gateway nos quais ele é implementado são processadores de HTTPS. O gateway utiliza diferentes métodos de comunicação, incluindo detecção de dispositivos, gerenciamento de eventos, coleta de dados de telemetria e gerenciamento de dados de telemetria. Os tipos de mensagem são:

- Consulta de heartbeat do estado do dispositivo
- Transferência de arquivos de dados (conexão com base)
- Transferência de dados de uso do licenciamento
- Solicitações de autenticação do usuário
- Sincronização do gerenciamento de dispositivos

Todas as mensagens são codificadas com segurança por meio de vários protocolos. Em uma próxima seção, analisaremos com detalhes a segurança adicional integrada à comunicação e ao transporte de dados do gateway de conexão segura, incluindo o uso do protocolo HTTPS com encapsulamento TLS completo e criptografia padrão do setor.

Controle do cliente de requisitos de autorização e permissões de acesso

Se os dispositivos são monitorados pelo gateway de conexão segura no data center de um cliente, ele pode optar por usar o gerenciador de políticas para controlar os requisitos de autorização para conexões de acesso remoto, execuções de scripts de diagnóstico e outras atividades relacionadas. Os clientes podem definir permissões de acesso para a equipe e os engenheiros de suporte técnico que se conectam remotamente para diagnosticar e corrigir problemas.

A segurança para gerenciamento de autorização e permissão é garantida pelas seguintes funções do gerenciador de políticas:

- O gateway de conexão segura faz consultas regulares ao gerenciador de políticas para verificar se existem alterações nas permissões e armazena as permissões em cache localmente. No caso do gerenciador de políticas:
  - O cache do conjunto de regras é atualizado automaticamente com as atualizações de configuração após o último ciclo da consulta.
  - Ele é configurado para receber mensagens como um ouvinte de HTTPS em uma porta específica e acordada.
- Quando o gateway de conexão segura recebe uma solicitação de acesso remoto ou qualquer outra ação, ele impõe a política recebida do cache do gerenciador de políticas.
  - As permissões podem ser atribuídas hierarquicamente com políticas baseadas em tipos de dispositivo ou em modelos específicos em um tipo de dispositivo.
  - Os clientes podem aceitar ou negar a ação solicitada por meio da interface do usuário da Web do geren-ciador de políticas. Eles também podem criar filtros para definir outras restrições de autorizações e ações.

Logs e trilhas de auditoria

Os clientes podem ter uma camada a mais de segurança para coleta de dados no local por meio dos recursos de auditoria do gerenciador de políticas no gateway de conexão segura. O gerenciador de políticas registra todos os eventos e conexões de serviços remotos, execuções de scripts de diagnóstico e operações de transferência de arquivos de suporte. Em seguida, ele os armazena em seu banco de dados como arquivos de log de auditoria em texto simples. Ele monitora o acesso a si mesmo (o gerenciador de políticas), as alterações de política e todas as atividades de autorização ou negação de acesso.

Os clientes têm todas essas informações ao seu alcance pois:

- As auditorias são visualizadas por meio da interface do usuário da Web do gerenciador de políticas e não podem ser editadas.
- Os logs de auditoria também podem ser configurados a fim de transmitir para um servidor syslog em seu ambiente.

Gateway de conexão segura

Suítes de criptografia TLS 1.2 compatíveis:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Opção de segurança do controle de dispositivo

Como os clientes nem sempre ativam o gerenciador de políticas para o gerenciamento de autorização e permissão, o gateway de conexão segura fornece recursos de segurança relacionados por meio da opção de controle do dispositivo.

Os clientes podem:

- Criar grupos personalizados com base no tipo de dispositivo, no grupo de administradores, na organização ou na unidade de negócios, no local físico do dispositivo ou em qualquer outro critério escolhido
- Definir permissões específicas e direitos de acesso por esses grupos de dispositivos

Todas as operações de gerenciamento de dispositivos, incluindo a atividade remota por engenheiros de suporte técnico, são registradas. Elas também devem ser aprovadas no back-end por um agente de suporte técnico.

Assim, os clientes mantêm total controle e transparência em relação aos dispositivos gerenciados por meio do gateway de conexão segura.

Autenticação de dois fatores e gerenciamento de certificado digital

A autenticação é um componente importante da coleta de dados segura no local. O gateway de conexão segura usa um certificado digital como prova de identidade de sua implementação no servidor de gateway do cliente. O certificado vincula a identidade do servidor de gateway a um par de chaves que é usado para criptografar e autenticar a comunicação com o back-end. A CA (Certificate Authority, Autoridade de Certificação) da Dell Technologies Services é o repositório central da infraestrutura de chave do gateway de conexão segura.

O gerenciamento do certificado digital é usado para automatizar a inscrição do certificado digital por meio de nossa autoridade de certificação privada. Isto:

- Permite a geração programática e a autenticação de cada solicitação de certificado.
- Garante que o certificado seja emitido e instalado apenas no servidor de gateway. O certificado não pode ser copiado e usado em outro computador.

O gateway de conexão segura se conecta e autentica usando o certificado digital implementado em nossa infraestrutura de suporte de back-end. Os agentes do suporte técnico se conectam ao gateway de conexão segura no ambiente do cliente usando a autenticação de dois fatores.

4-2: Transporte e comunicação seguros de dados

Túnel de comunicação seguro

Todas as comunicações entre o cliente e a infraestrutura do suporte de back-end da Dell Technologies Services são iniciadas pelo gateway de conexão segura a partir do local do cliente. Ele cria um túnel de comunicação seguro completo usando a criptografia TLS de 256 bits padrão do setor pela Internet e a autenticação de certificado digital assinada pela Dell Technologies Services. Essa autenticação é detalhada na seção anterior, que aborda a coleta de dados segura no local.

Como resultado, as conexões do gateway de conexão segura têm as seguintes propriedades:

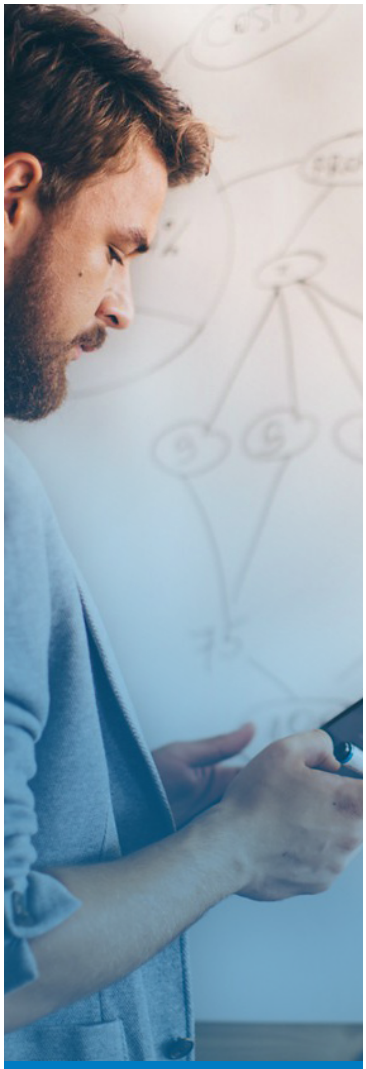
- **Transferência de dados confiável:** cada mensagem transmitida inclui uma verificação de integridade de mensagem usando um código de autenticação para evitar perda ou alteração não detectada dos dados durante a transmissão.
- **Sessão privada e segura por TLS:** a criptografia simétrica que usa algoritmos padrão do setor gera chaves exclusivas para cada conexão. As comunicações não podem ser modificadas durante a negociação sem serem detectadas.
- **Partes autenticadas:** como a conexão é segura, ele identifica as partes comunicantes e as autentica usando criptografia de chave pública. Essa abordagem evita ataques de spoofing e do tipo man-in-the-middle (MITM).

Comunicações usando o túnel TLS seguro

O servidor de gateway usa o túnel TLS para garantir um ambiente seguro para as seguintes funções: consulta de heartbeat, notificação remota e acesso remoto. Nesta seção e, de acordo com o Diagrama C, analisamos detalhadamente esses processos e protocolos de comunicação essenciais para a experiência automatizada, proativa e preditiva da nossa tecnologia.

Consulta de heartbeat

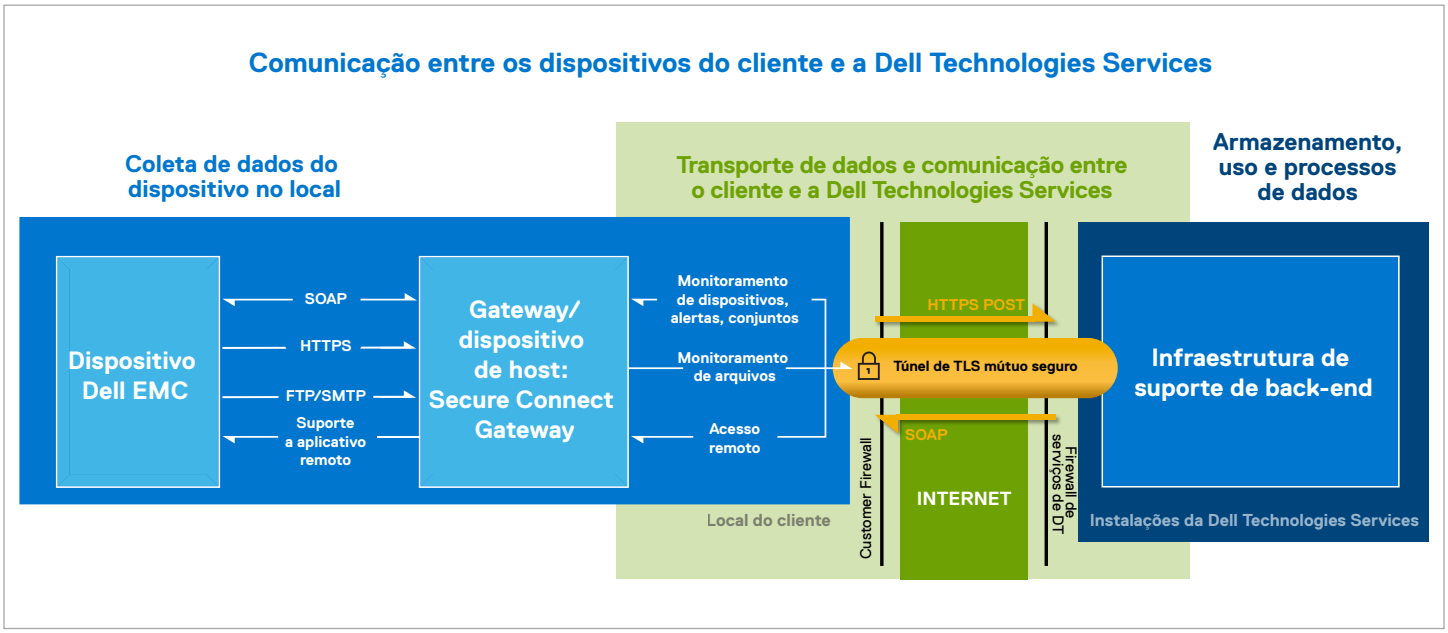
Os sistemas do cliente precisam estar conectados para que você aproveite a experiência do gateway de conexão segura. A consulta de heartbeat verifica o status de conectividade dos dispositivos e transmite regularmente os dados de telemetria coletados para o back-end. Os dados também identificam o servidor de gateway no qual o gateway de conexão segura está implementado.



A autenticação líder do setor protege as conexões contra falsificação e ataques do tipo “man-in-the-middle”

Comunicações usando o túnel de TLS seguro continuaram

Diagrama C: arquitetura de segurança



Notificação remota ou função de conexão com base

O gateway de conexão segura funciona como um conduíte seguro para que os dispositivos enviem arquivos de eventos ao back-end. Alguns exemplos são erros, alertas, condições de advertência, relatórios de integridade, dados de configuração e status de execução de scripts.

- Quando um alerta é gerado, um arquivo de evento é gerado e enviado para o gateway.
- O arquivo é recebido pelo gateway de conexão segura pelos serviços de escuta de HTTPS.
- No caso de produtos preexistentes que usam escutas de FTP e/ou SMTP para o gateway de conexão segura, os arquivos são criptografados e transferidos.
- O gateway compacta o arquivo e o envia para o back-end pelo túnel de TLS. Em seguida, exclui o arquivo do diretório de escuta.
- Em seguida, o arquivo é descompactado no back-end para análise.
- O gateway de conexão segura também pode enviar os arquivos para o back-end pelo túnel de comunicação criptografado. Além disso, o gateway pode ser configurado para usar os canais de failover, ou seja, o FTPS ou o servidor de e-mail do cliente.

Os dados de monitoramento do sistema são coletados de vários componentes de um sistema ativo para permitir que a Dell Technologies Services ofereça uma experiência de suporte adaptável, inteligente e acelerada. O ID do sistema, necessário para identificar o sistema específico que está sendo trabalhado, é a única informação sobre a empresa coletada dos dispositivos. Quando determinamos que uma peça deve ser enviada proativamente, usamos as informações de contato existentes armazenadas com segurança nos servidores da Dell Technologies.

Uma lista completa dos dados de monitoramento do sistema que são coletados de um sistema ativo, que inclui dados coletados fora do ciclo rotineiro de 24 horas, está disponível nos documentos Itens reportáveis do Gateway de conexão segura e do plug-in de Serviços para OpenManage Enterprise.

Acesso remoto

Nossas equipes de suporte técnico também acessam os dispositivos remotamente no local do cliente para solucionar problemas ou executar ações específicas do dispositivo. O sistema de mensagens assíncronas garante que a sessão de acesso remoto seja iniciada pelo gateway de conexão segura no local do cliente. Em seguida, uma sessão segura de acesso remoto é estabelecida da seguinte maneira:

- Após a autenticação da sessão no back-end da Dell Technologies Services, um agente de suporte técnico solicita o acesso do dispositivo, incluindo o número do chamado, se disponível, e outros identificadores de dispositivo ou de usuário.
- A solicitação de acesso remoto é colocada na fila do back-end até que o gateway envie a mensagem de heartbeat do dispositivo ao back-end para recuperá-la.
- Em resposta, o servidor de back-end envia uma resposta que inclui informações de solicitação, o endereço do servidor de back-end e um ID de sessão exclusivo para a conexão com o gateway.
- O gateway de conexão segura usa seu repositório local para determinar o endereço IP local do dispositivo. Em seguida, ele verifica a política de cache do gerenciador de políticas para autorizar as permissões de conexão.
- Se permitido, o gateway de conexão segura estabelece uma conexão TLS persistente separada para o servidor de back-end. A conexão TLS é sempre iniciada pelo gateway. O servidor back-end nunca pode iniciar uma conexão de entrada com o servidor de gateway. Isso garante que não haja vulnerabilidades a ataques externos.

A comunicação flui pelo túnel entre o gateway de conexão segura e o servidor de back-end até que seja encerrada ou que o tempo de espera seja excedido após um período de inatividade.

Segurança de rede

Todos os componentes de monitoramento de rede são protegidos por um firewall e gerenciados pela nossa equipe de segurança de rede. O tráfego de rede é totalmente controlado. Todo o tráfego de entrada é transmitido por portas específicas e é enviado apenas para endereços de rede de destino apropriados.

4-3: Armazenamento, uso e processos seguros de dados

Segurança para armazenamento e uso

Segurança física

A Dell Technologies Services hospeda a maior parte dos dados do gateway de conexão segura, incluindo aplicativos, sistemas, rede e componentes de segurança, em um data center localizado nos EUA que foi criado para manter altos níveis de disponibilidade e segurança. Os dados são protegidos por uma ampla variedade de medidas, incluindo segurança física. Os recursos incluem, entre outros:

- Profissionais de segurança no local
- Câmeras
- Entradas falsas
- Bloqueios de veículos
- Design de estacionamento especializado
- Vidro e paredes à prova de balas
- Uso de um prédio não marcado

O acesso aos data centers em que a infraestrutura reside está restrito a pessoas autorizadas. O acesso é controlado por meio de smart card.

Segurança lógica

Os dados gerados pelo gateway de conexão segura são armazenados em conformidade com a Política de privacidade da Dell.

O acesso lógico à infraestrutura da Dell Technologies Services (servidores, balanceadores de carga, compartilhamentos de rede etc.) é restrito por meio de ferramentas internas que são auditadas e avaliadas de acordo com as diretrizes de TI:

Segurança lógica continuada

- **Segurança de servidor e banco de dados:** os servidores e os componentes do sistema operacional residem em imagens padrão que foram submetidas a análises de segurança. Há revisões regulares das atualizações de segurança usadas pelo aplicativo, incluindo as publicadas pela Microsoft e outros fornecedores de software. Quando as atualizações de segurança críticas são emitidas, primeiro elas são testados em imagens não utilizadas na produção e, em geral, são aplicadas em servidores dinâmicos em tempo hábil para evitar riscos.
- **Auditoria:** os logs de dispositivos monitorados são mantidos, com acesso somente pelos aplicativos e a infraestrutura autorizados da Dell Technologies Services. Esses logs registram todas as tentativas de login ou de acesso ao sistema operacional ou ao console do servidor da Web do gateway de conexão segura.

As compilações gerenciadas pela equipe de TI são reforçadas pelas recomendações do CIS (Center for Internet Security). As diretrizes de segurança padrão do setor também são implementadas em todos os servidores e equipamentos de rede.

Por fim, o ecossistema do gateway de conexão segura utiliza a alta disponibilidade local em seu data center e a infraestrutura idêntica em um data center separado. As únicas exceções são as tecnologias que são intrinsecamente de alta disponibilidade, como clusters de big data e nuvens privadas. Para a lógica analítica de dados, a Dell Technologies Services utiliza ambientes de nuvem que controlamos e gerenciamos por completo, incluindo nuvens privadas, híbridas e públicas.

Autenticação

O gateway de conexão segura usa o Dell MyAccount para autenticação na Dell Technologies Services e grupos de login do OS para uma autenticação imediata.

Os grupos que têm acesso aos componentes do gateway de conexão segura, como a equipe de administração do banco de dados e a equipe de suporte operacional, recebem tarefas e direitos de acesso separados. Todas as atualizações no ambiente de produção passam por um processo definido de controle de alterações que incorpora verificações e balanços.

Segurança para processos

Comunidade com reconhecimento de segurança

Oferecemos um currículo de treinamento de segurança baseado em funções de vários níveis para treinar funcionários novos e antigos sobre as práticas recomendadas de segurança específicas do trabalho e como usar os recursos relevantes. A Dell Technologies se esforça para criar uma cultura atenta à segurança em toda a comunidade. Além disso, nossa comunidade de desenvolvedores faz parte do programa Security Champion da Dell, criado para incentivar a segurança em nossas práticas de desenvolvimento de software.

Utilizamos um processo de desenvol-vimento seguro e que pode ser repetido para produtos e aplicativos

Desenvolvimento

Nossa **norma interna de SDL (Secure Development Lifecycle, Ciclo de Vida de Desenvolvimento Seguro)** é uma referência comum às organizações de produtos da Dell Technologies para ter as referências de desempenho das atividades de desenvolvimento seguro de produtos e aplicativos em relação às expectativas do mercado e às práticas do setor. Ela define controles de segurança que as equipes de produtos devem adotar durante o desenvolvimento de novos recursos e funcionalidades. O SDL inclui as atividades de análise e os controles proativos prescritivos relacionados às principais áreas de risco. As atividades de análise, como modelagem de ameaças, análise de código estático, digitalização e testes de segurança, têm a finalidade de detectar e solucionar defeitos de segurança durante todo o ciclo de vida do desenvolvimento. Os controles prescritivos devem garantir que as equipes de desenvolvimento codifiquem de forma defensiva para evitar problemas de segurança predominantes específicos, incluindo os encontrados no Open Web Application Security Project (OWASP) Top 10 ou no SANS Top 25. O gateway de conexão segura adotou

Desenvolvimento contínuo

a estrutura de maturidade do SDL da Dell para implementar controles de segurança em alinhamento com os padrões do setor.

O código do gateway de conexão segura é desenvolvido com a metodologia de desenvolvimento ágil. O código é integrado continuamente usando software de automação padrão do setor. As versões de código são verificadas e controladas com as permissões de grupo seguro.

Todas as versões de software passam por uma avaliação de segurança de acordo com nossas políticas de segurança e incluem:

- Avaliação de vulnerabilidade usando testes de penetração
- Teste de segurança de terceiros usando vários dos melhores fornecedores da categoria, como a Secureworks
- Avaliação de autenticação, autorização e soluções de gerenciamento de identidade
- Todas as bibliotecas e componentes de terceiros são examinados com as soluções líderes do setor para análise da composição do software. Além disso, consultores de segurança da Dell são comunicados para realizar melhorias de segurança específicas.
- Classificação de dados com a nossa organização global de segurança. Esse processo reúne a privacidade e a segurança para garantir a proteção dos dados eletrônicos.

Os aplicativos também são submetidos a auditorias de segurança e governança.

Gerenciamento de mudanças

O processo de gerenciamento de mudanças da Dell Technologies segue as melhores práticas da ITIL Foundation, conforme determinado pela nossa diretoria de gerenciamento de mudanças corporativas. Todas as mudanças são gerenciadas por meio de tíquetes de solicitação de alteração. Aqueles que acessam o nosso sistema para iniciar mudanças devem passar pelo treinamento em ITIL, assim como se familiarizaram com o SDL. Todas as atualizações e upgrades aplicados à infraestrutura de back-end têm versão controlada para fins de rastreamento e acompanhamento. A equipe emprega um processo de criação automatizado para aplicar novas compilações ou revogar qualquer compilação ou hotfix implementada.

O aplicativo instalado no local do cliente pode receber um upgrade com base na preferência dele. Todas as versões promovidas em Dell.com/support contêm informações sobre as alterações introduzidas com quaisquer limitações conhecidas.

Todos os novos recursos e alterações são preparados pela nossa equipe de gerenciamento de produtos e são priorizados com o uso de um processo de alteração do plano de registro, que é analisado e aprovado pelo controle de alterações.

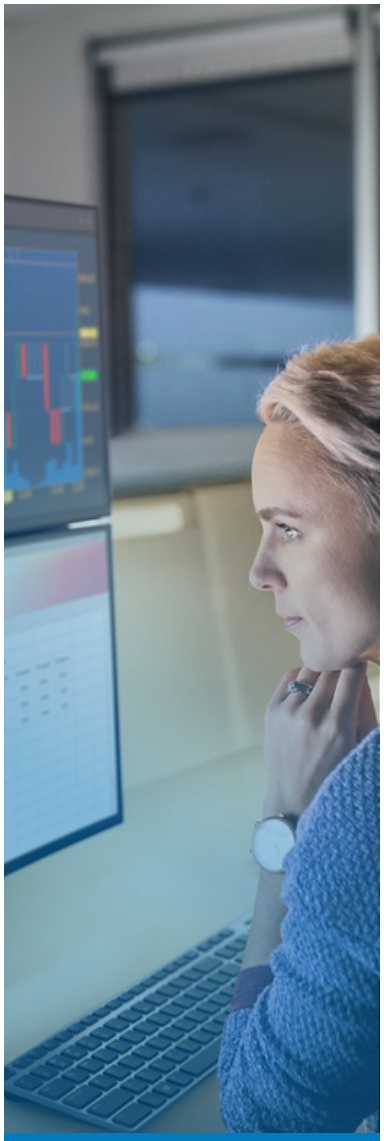
Gerenciamento do risco da cadeia de suprimentos

A Dell Technologies segue as melhores práticas líderes do setor em cada etapa do ciclo de vida útil de planejamento-fonte-produção-entrega-devolução. Adotamos uma abordagem abrangente a fim de proteger nossa cadeia de suprimentos, incluindo a adoção de padrões e melhores práticas internacionais de SCRM para continuar sendo um fornecedor de TIC confiável no mercado global.

Saiba mais sobre nossas práticas de garantia da cadeia de suprimentos aqui.

Geração de relatórios de incidentes

Todo funcionário da Dell Technologies que observa uma atividade suspeita ou suspeita de um problema ou ameaça de segurança cibernética precisa relatar o incidente imediatamente para a CSIRT (Computer Security Incident Response Team, Equipe de Resposta a Incidentes de Segurança do Computador). Essas ameaças podem ser pontos fracos ou lacunas de um processo de segurança que possam afetar nosso ambiente ou causar uma violação de sistemas e/ou dados. Depois, a CSIRT inicia uma investigação completa do incidente, e a pessoa que relatou o incidente apresenta todos os fatos e detalhes necessários para que a CSIRT faça a investigação. A CSIRT usa o Plano de resposta a incidentes, que detalha um processo formal para responder e resolver os incidentes internos de segurança cibernética da Dell que não chegam aos clientes. Esses incidentes podem representar ameaças potenciais não só para os ativos, as redes de computadores ou os equipamentos de processamento de dados da Dell, mas também para as informações de suas subsidiárias, equipes, fornecedores de serviços, parceiros ou clientes aplicáveis.



Colaboração do setor sobre as melhores práticas de segurança do produto

Resposta da vulnerabilidade

A Dell Technologies procura ajudar os clientes a minimizar o risco associado às vulnerabilidades de segurança em nossos produtos fornecendo aos clientes informações oportunas, orientação e redução para lidar com as ameaças de vulnerabilidades. Nossa PSIRT (Product Security Incident Response Team, Equipe de Resposta a Incidentes de Segurança de Produtos) é responsável por coordenar a resposta e a divulgação de todas as vulnerabilidades de produtos relatadas para nós. Todas as divulgações de vulnerabilidade de produtos Dell Technologies estão disponíveis on-line.

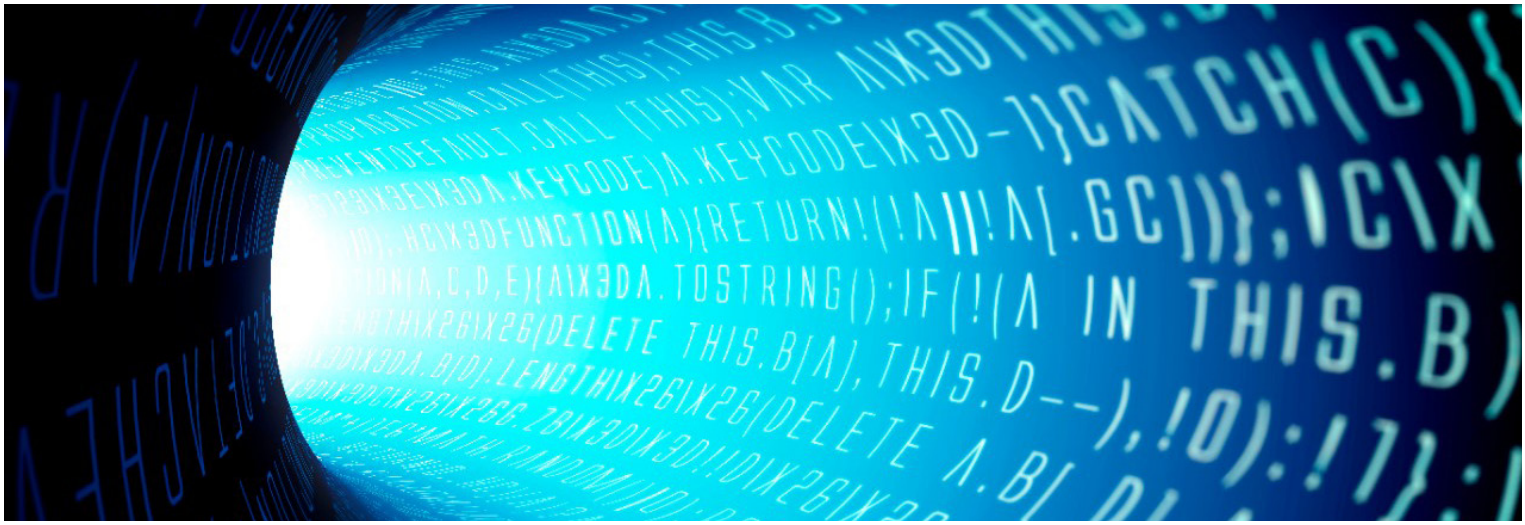
Saiba mais sobre a nossa Política de resposta à vulnerabilidade

Afiliações do setor

A Dell Technologies participa de vários grupos de todo o setor para colaborar com outros fornecedores líderes na definição, na evolução e no compartilhamento das melhores práticas de segurança do produto e na melhoria da causa do desenvolvimento seguro. Os exemplos de colaboração no setor incluem:

- A Dell, por meio de sua entidade EMC, participou da fundação e atualmente preside a diretoria do The Software Assurance Forum for Excellence in Code (SAFECode). Outros membros do conselho incluem representantes da Microsoft, Adobe, SAP, Intel, Siemens, CA e Symantec. Os membros do SAFECode compartilham e publicam práticas e treinamentos de garantia de software.
- A Dell Technologies é um membro ativo do The Forum for Incident Response and Security Teams (FIRST). O FIRST é uma organização reconhecida e uma líder global de resposta a incidentes e vulnerabilidades.
- Participamos ativamente do Open Group Trusted Technology Forum (OTTF). O OTTF lidera o desenvolvimento de um programa e estrutura de integridade da cadeia de suprimentos global.
- A Dell foi uma das primeiras nove empresas avaliadas pelo projeto Building Security In Maturity Model (BSIMM) em 2008 e continuou a participar do projeto. Um representante da Dell Technologies faz parte do conselho consultivo do BSIMM.
- Os funcionários da Dell foram membros fundadores do IEEE Center for Secure Design, que foi lançado sob a iniciativa de segurança cibernética da IEEE para ajudar os arquitetos de software a compreender e lidar com falhas de design de segurança predominantes.

Acesse nossa Central de confiabilidade e segurança para conferir recursos e soluções que podem ajudar você a encontrar as respostas às suas perguntas sobre segurança empresarial.



Padrões de segurança do setor

Nossos funcionários estão envolvidos ativamente em órgãos de normas e em consórcios do setor, que se concentram no desenvolvimento de padrões de segurança e na definição de práticas de segurança em todo o setor incluindo:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- The Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Certificação ISO 9001

A Dell Technologies tem a certificação ISO 9001. A empresa realiza auditorias trimestrais regulares e análise de conformidade para todos os seus centros de desenvolvimento e fabricação.

5: conclusão

Nossa tecnologia de conectividade oferece uma experiência de suporte de TI sem dificuldades, com alertas proativos e preditivos automatizados que garantem o máximo de tempo de funcionamento para a infraestrutura essencial de um data center. Os clientes parceiros da Dell Technologies Services podem ter a certeza do nosso compromisso de oferecer uma experiência confiável, segura e privada para a coleta, a comunicação, o transporte, o uso e o armazenamento de seus dados de telemetria.

Em caso de dúvidas e para obter mais informações, acesse DellTechnologies.com/SecureConnectGateway

1 Fonte: "The Role Of IT Services Providers Expands To Strategic Collaboration", um estudo comissionado realizado pela Forrester Consulting em nome da Dell Technologies, abril de 2021

2 Fonte: World Economic Forum Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf