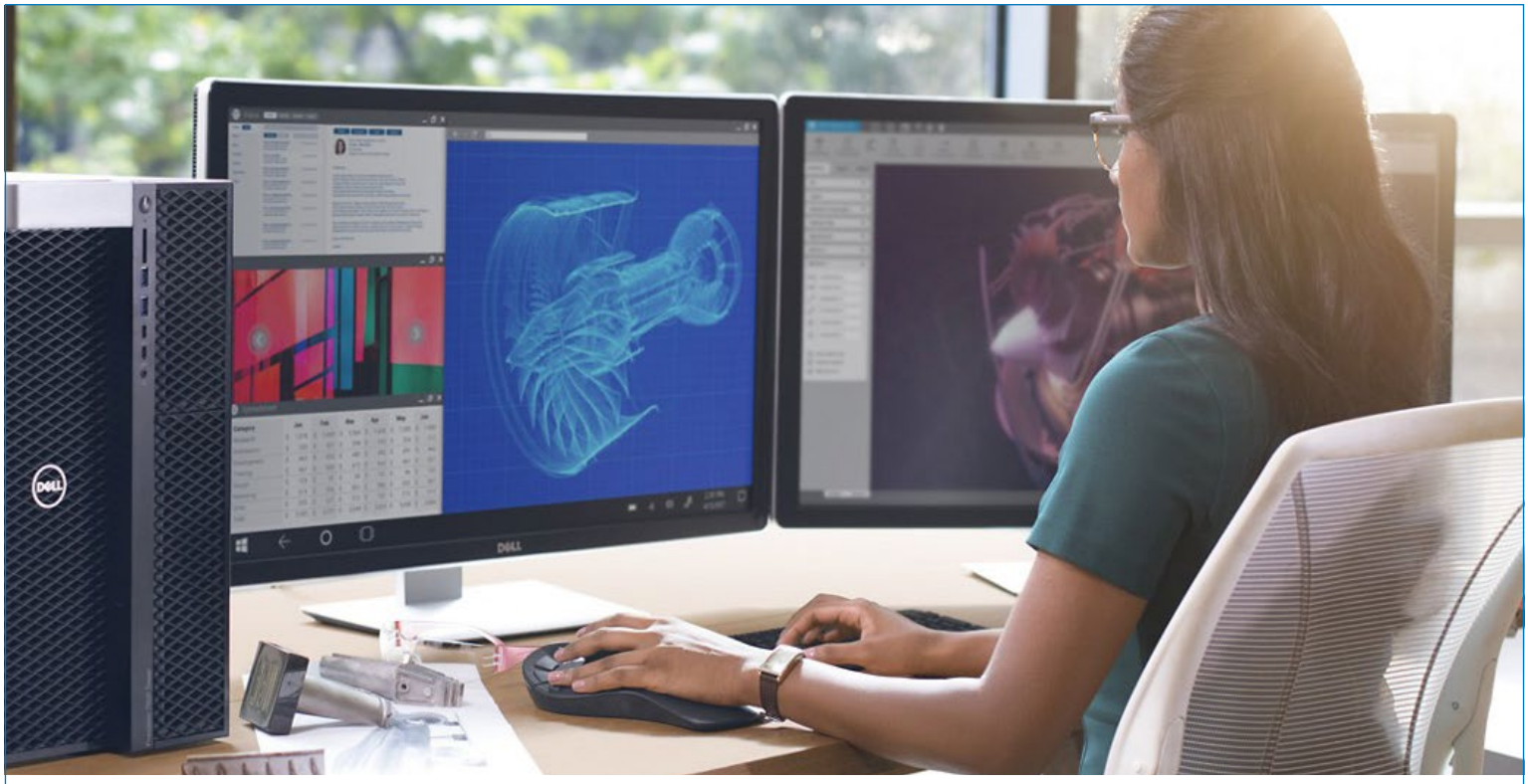
SupportAssist for Business PCs: Visão geral de segurança

Cinco perguntas-chave sobre a segurança do SupportAssist — e suas respostas.

O SupportAssist permite automatizar o suporte da Dell Technologies ao identificar problemas de hardware e software em todo o parque de PCs. O SupportAssist resolve problemas de desempenho e estabilização do sistema, reduz ameaças à segurança, monitora e detecta falhas de hardware e automatiza o processo de engajamento com o suporte técnico da Dell.

O SupportAssist também coleta proativamente dados de telemetria dos PCs e fornece insights da utilização do PC com base no plano de serviço.



Conteúdo

I: Introdução

Falhas no notebook causam disrupção e frustração. Esses problemas podem afetar severamente a produtividade do funcionário e, muitas vezes, no pior momento possível. Por isso, os CIOs corporativos estão cada vez mais preocupados com a qualidade e o tempo de funcionamento dos parques de computadores.

Muitos recorrem à tecnologia mais recente e avançada, que usa insights da ciência de dados para processar bilhões de pontos de dados e ajudar os administradores de TI a serem mais eficientes. Isso é feito enviando informações de estado dos sistemas do usuário final ao departamento de TI da empresa ou a um fornecedor de hardware ou software para resolver os problemas assim que eles acontecem ou impedir que aconteçam. O Dell ProSupport Plus com tecnologia de conectividade SupportAssist alerta sobre falhas no disco rígido, fornecendo uma visão única de todo o parque de PCs no portal TechDirect.

Embora essa tecnologia seja necessária para garantir o tempo de funcionamento e a eficiência, os CIOs às vezes têm dúvidas sobre as informações coletadas e como elas são tratadas.

As perguntas a seguir são consideradas essenciais:

- Quais dados o SupportAssist coleta?
- Como esses dados são protegidos ao serem transmitidos de volta para o departamento de TI da empresa ou para o fornecedor de computadores?
- Assim que chegam ao destino, os dados são armazenados de maneira que permaneçam privados e protegidos?

Este artigo avalia essas e outras questões relacionadas como um meio de avaliar tecnologias habilitadas para ciência de dados. Ele fornece uma breve visão geral de como o SupportAssist oferece o ProSupport Suite for PCs como um serviço de suporte completo capaz de prever e corrigir problemas antes que eles agravem. Ele também apresenta um panorama detalhado de como a Dell Technologies Services protege dados confidenciais durante os processos, o transporte e o armazenamento de dados.

II: Sobre o SupportAssist

O SupportAssist é nossa tecnologia de conectividade inteligente[1] que possibilita à organização receber suporte técnico automatizado para todo o parque de PCs. Ele monitora os dispositivos do usuário final, detecta proativamente problemas de hardware e software e fornece insights sobre o uso do sistema.

Quando detecta um problema, o SupportAssist abre automaticamente uma solicitação com o suporte técnico. Dependendo do tipo de problema, o alerta pode iniciar uma solicitação de suporte técnico ou um despacho automático de peças. O SupportAssist coleta dados de hardware e software que são usados pelo suporte técnico para solucionar o problema.

O Dell ProSupport Suite for PCs oferece os recursos de suporte mais abrangentes em uma única solução, sem a necessidade de adicionar mais serviços[2]. Saiba mais.

Principais recursos

- Detecção proativa e preditiva de todo o parque para mais rapidez na resolução de problemas
- Análise rápida de pontuações de integridade, segurança e experiência nos aplicativos em uma só tela
- Regras personalizadas que definem os fluxos de trabalho de correção
- Automatização da criação e da implementação de catálogos de atualização personalizados para BIOS, drivers, firmware e aplicativos Dell
- Flexibilidade para adaptar exibições e painéis de indicadores no TechDirect

Os recursos disponíveis variam com base no plano de suporte adquirido para o PC.

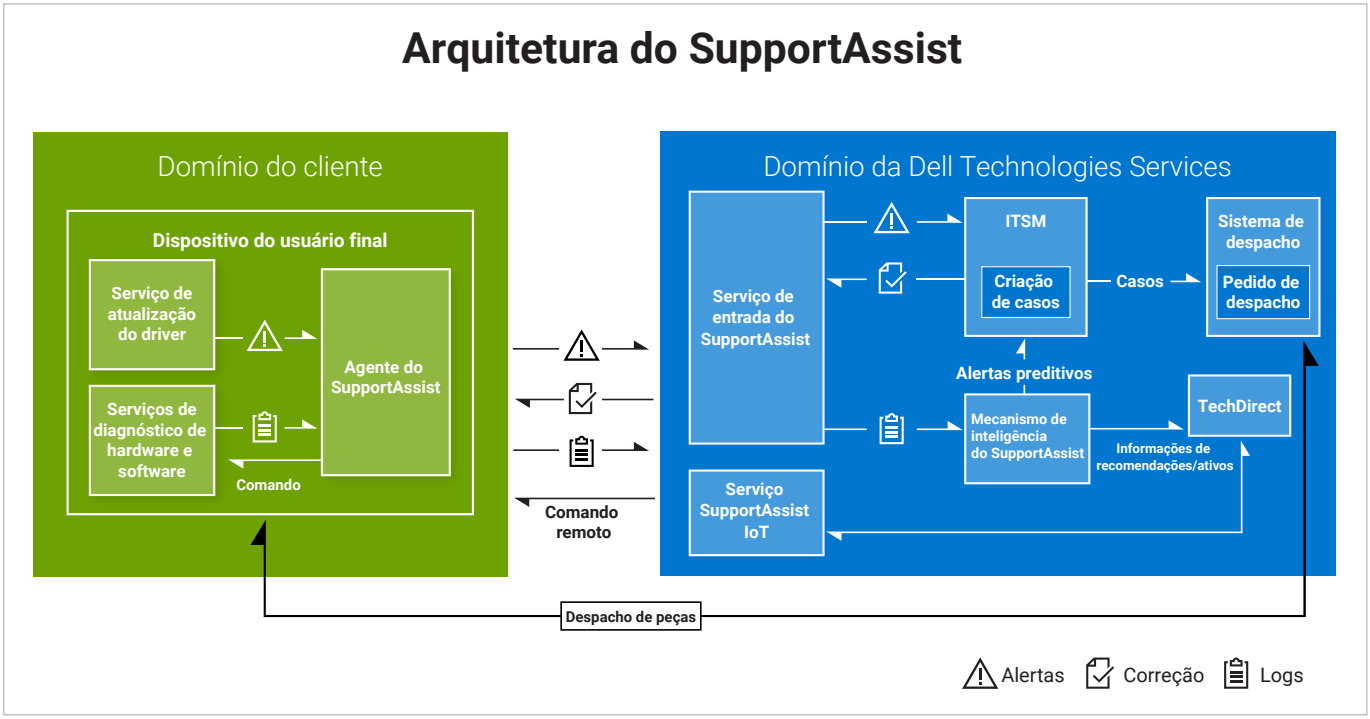
- Com o ProSupport Plus, os usuários finais recebem um conjunto completo de recursos do SupportAssist, incluindo detecção preditiva de problemas e prevenção de falhas.

Para obter uma lista completa de recursos e funcionalidades, consulte nosso Guia do administrador.

III. Arquitetura do SupportAssist

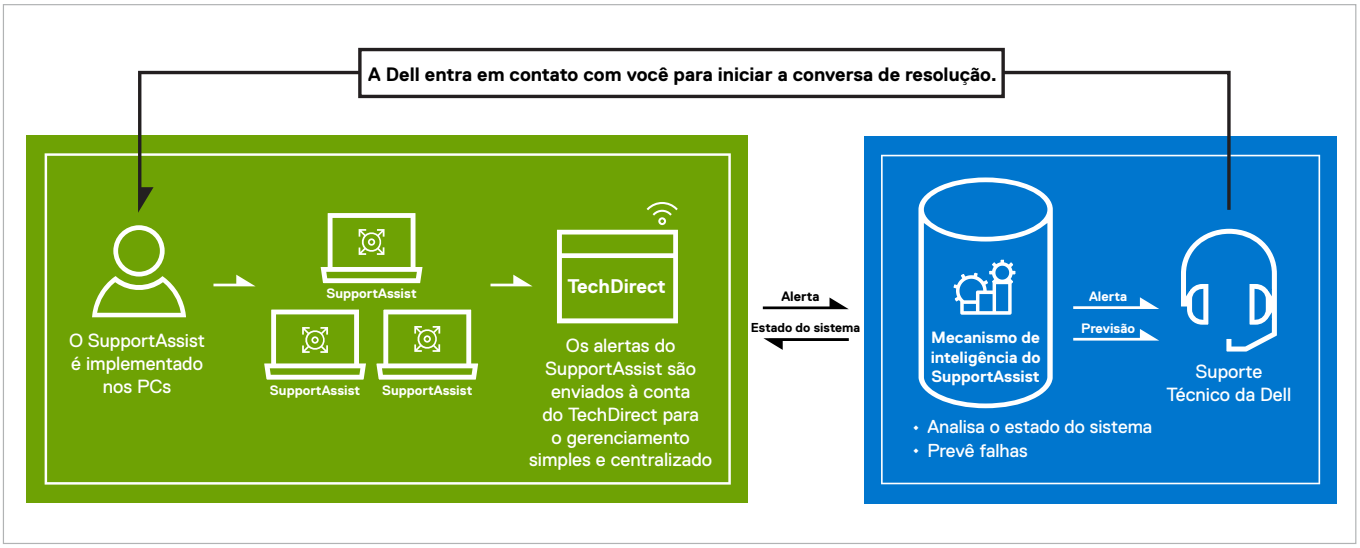
O SupportAssist compreende um conjunto de serviços que monitora continuamente os sistemas e executa verificações de integridade com base em programação no dispositivo. Essas informações são transmitidas aos servidores da Dell Technologies para análise dos dados e recomendações.

Para obter uma lista completa dos requisitos de rede, endpoint, portas, firewall ou gateway para implementação e correção do SupportAssist, consulte nosso Guia de implementação. Nossos scripts de correção foram desenvolvidos, testados e assinados pela Dell e depois confirmados antes da execução.



Gerencie o SupportAssist de modo centralizado usando o TechDirect

Os alertas do SupportAssist podem fluir para a conta do TechDirect da organização, o que possibilita um gerenciamento conveniente e centralizado. As organizações com um plano de serviço ProSupport ou ProSupport Plus também podem optar por encaminhar automaticamente alertas para a Dell Technologies Services.

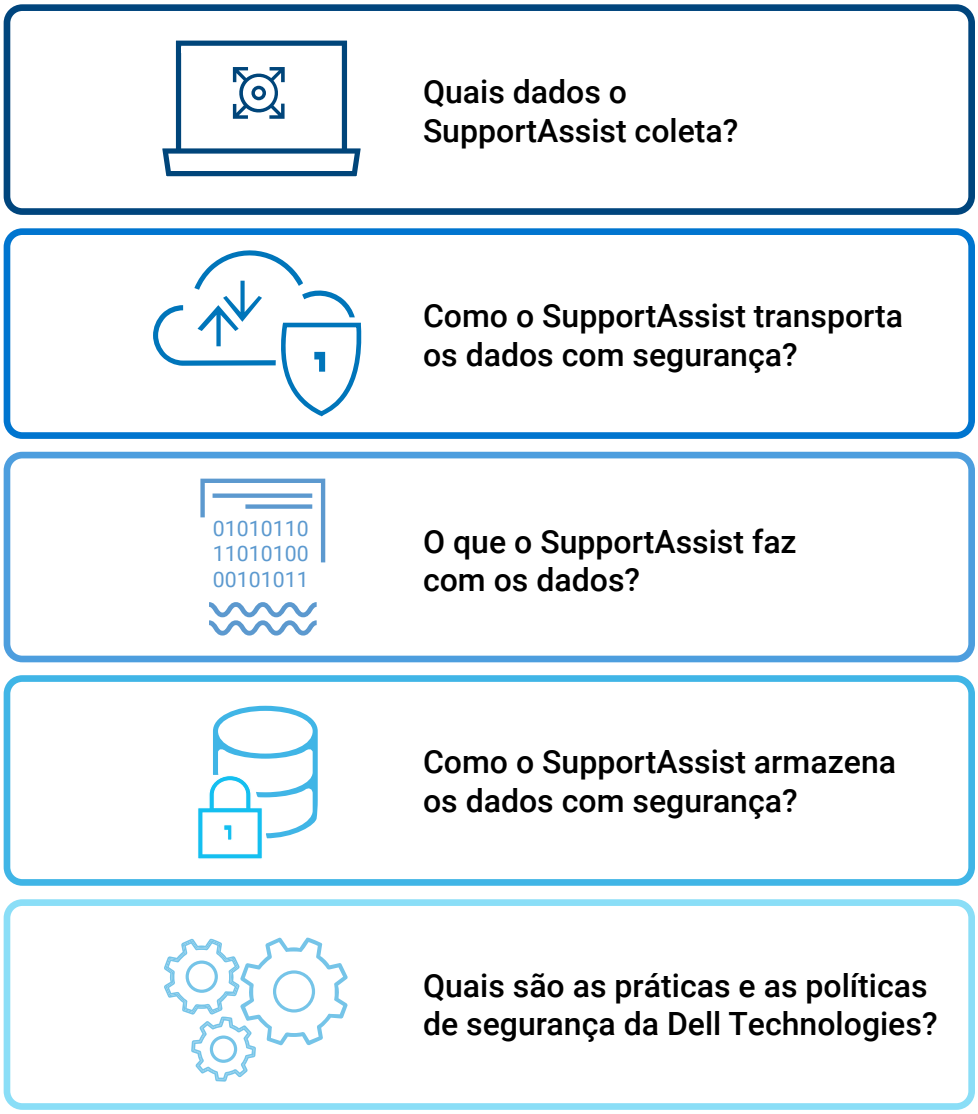


Gerencie o SupportAssist de modo centralizado usando o TechDirect (continuação):

O Insights do SupportAssist, um componente analítico muito útil, coleta dados de utilização do sistema que podem ser visualizados no console do TechDirect. Eles incluem utilização da CPU, espaço livre na unidade, capacidade máxima da bateria, tempo de execução da bateria e muitos outros insights úteis. O TechDirect pode exibir essas informações referentes a todos os sistemas, a sistemas em um grupo de dispositivos específico ou a um sistema individual. Os clientes são capazes de identificar problemas de desempenho e tomar decisões de negócios melhores (por exemplo, atualizar ou substituir um hardware).

IV. Segurança do SupportAssist

O CIO ou CSO de uma organização pode ter as seguintes dúvidas sobre quais tipos de dados são coletados pelo SupportAssist for Business PCs e como são processados. Esta seção responderá a essas perguntas, mostrando como o SupportAssist coleta apenas os dados necessários para corrigir problemas do cliente e, em seguida, processa esses dados priorizando a segurança.



Quais dados o SupportAssist coleta?

O SupportAssist coleta automaticamente os dados necessários para solucionar um problema e os envia com segurança para o suporte técnico. Com esses dados, podemos oferecer uma experiência de suporte adaptável, inteligente e acelerada.

A etiqueta de serviço, necessária para identificar o dispositivo do usuário final específico em que estamos trabalhando, é a única informação sobre a empresa coletada dos dispositivos. Quando o SupportAssist determina que uma peça deve ser enviada proativamente, usamos as informações de contato existentes armazenadas com segurança nos servidores da Dell Technologies.

As seguintes informações do sistema são coletadas e enviadas uma vez a cada 24 horas como parte do monitoramento de rotina do sistema:

- **Versão do esquema:** Versão do esquema usado para o monitoramento de rotina do sistema
- **Versão do agente:** Versão do SupportAssist implementada no sistema
- **Etiqueta de serviço:** Identificador exclusivo do sistema
- **Modelo do sistema:** Nome do modelo do sistema
- **Informações de registro:** Status de registro do SupportAssist
- **Versão do sistema operacional:** Versão do sistema operacional em execução no dispositivo
- **Versão do SP:** Pacote de serviços do sistema operacional
- **Data UTC:** Data e hora em que as informações rotineiras de monitoramento do sistema foram enviadas à Dell Technologies Services
- **Versão do BIOS:** Versão do BIOS instalada no sistema
- **Status:** Status do alerta dependendo da severidade, por exemplo, advertência
- **Descrição:** Informações sobre a falha do sistema, por exemplo, alto uso da CPU
- **Espaço livre no disco rígido:** Espaço livre disponível no disco rígido do sistema
- **Uso da memória:** Quantidade de memória do sistema utilizada
- **Uso da CPU:** Quantidade de CPU utilizada
- **Data local:** Data e hora do sistema
- **Data da última inicialização:** Data e hora em que o sistema foi reiniciado pela última vez
- **Data de execução da atualização do Windows:** Data e hora em que o Windows foi atualizado pela última vez no sistema
- **Contagem de BSOD em 24 horas:** Número de ocorrências de tela azul nas últimas 24 horas
- **Informações do alerta:** Identificador exclusivo do alerta

Para obter mais informações sobre os dados de monitoramento coletados de um sistema ativo, acesse nossa página Dell.com aqui.

Todas as informações são transmitidas por canais seguros.

Como o SupportAssist transporta dados com segurança?

Os dados enviados do SupportAssist para a Dell Technologies Services usam criptografia de 256 bits e são transferidos com segurança usando o protocolo TLS.

Uma chave de criptografia é gerada no tempo de execução em cada máquina durante a instalação do pacote. A chave de criptografia, junto com o salt, é usada para criptografar as informações instaladas. Um algoritmo padrão do setor é usado para criptografar dados em repouso.

Na criptografia, salt são dados aleatórios usados como entrada para uma função unidirecional que aplica hash nos dados, na senha ou na frase secreta. A principal função dos salts é defender contra ataques de dicionário ou contra o equivalente com hash, um ataque pré-calculado de tabela arco-íris.

Todas as chaves de criptografia são criadas usando geradores de números aleatórios seguros. Os dados em trânsito são protegidos usando TLS sobre Hypertext Transfer Protocol Secure (HTTPS). Todos os algoritmos de criptografia são padrão do setor, e os dados em repouso são criptografados.

O HTTPS é usado em comunicações de saída para transmissões de feedback fornecido pelo usuário, eventos de telemetria de diagnóstico e consulta de uma API em Dell.com ou no Microsoft Azure IoT Hub para obter informações do sistema usadas no processo de restauração. Um MQTT seguro é usado para a abordagem pub-sub.

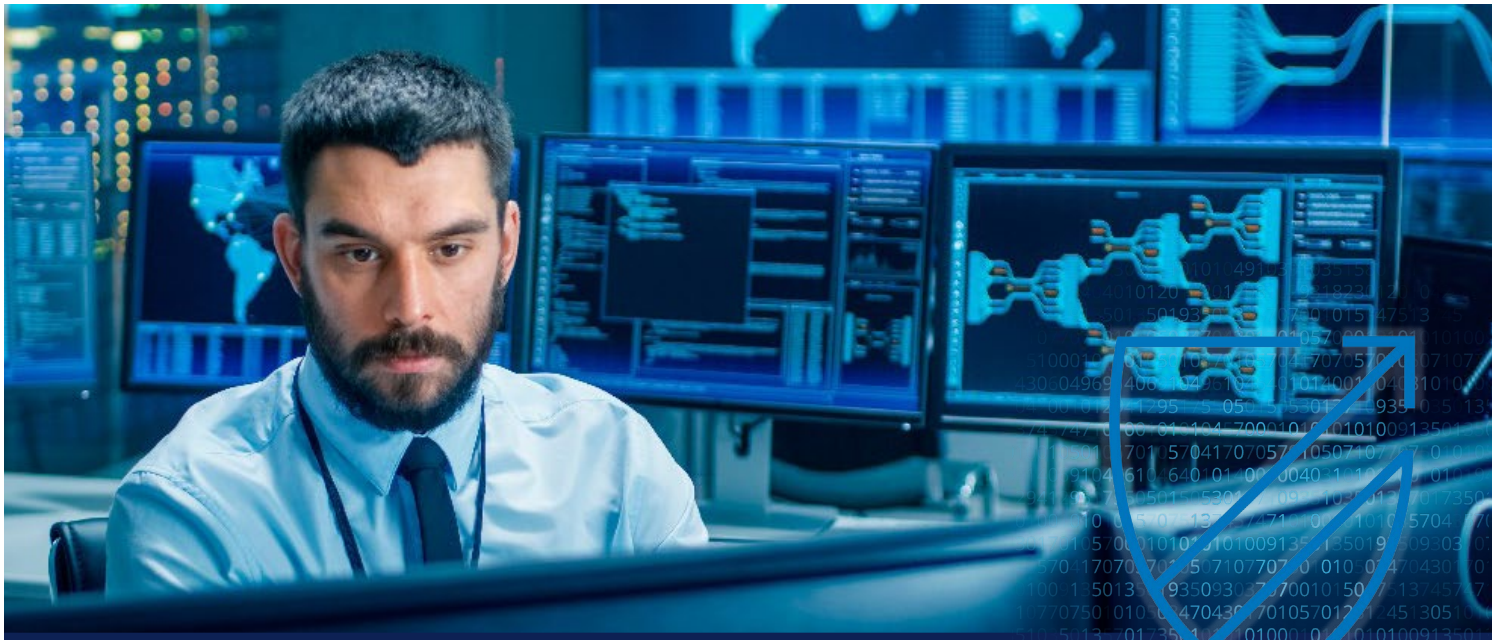
O HTTPS padrão é usado para proteger as comunicações entre o cliente e a infraestrutura de back-end ao transmitir ou fazer download de conteúdo para o dispositivo do usuário final. O HTTPS ou MQTT seguro é usado para a transmissão segura de dados de telemetria, a comunicação com uma API de back-end em Dell.com ou no Microsoft Azure IoT Hub e o download de conteúdo recuperado de Dell.com.

Todos os componentes de rede estão localizados atrás de um firewall e são gerenciados por uma equipe de segurança de rede. O tráfego de rede é rigidamente controlado. Todo o tráfego de entrada é transmitido por portas específicas e enviado apenas para endereços de rede de destino apropriados. O SupportAssist utiliza a largura de banda da rede para vários eventos que exigem conectividade com a infraestrutura da Dell Technologies Services. A largura de banda utilizada pode variar de acordo com o número de sistemas de destino monitorados pelo SupportAssist. A Tabela 1 fornece a largura de banda média de rede que o SupportAssist utiliza para monitorar um único PC.

Tabela 1. Consumo médio de dados

Evento	Frequência do evento	Consumo de dados por PC
Registro do SupportAssist	Uma vez após a implementação	15 KB
Envio de informações do PC ou dados mínimos de telemetria	Uma vez a cada 6–24 horas	4 KB
Carregamento de informações do PC durante varreduras agendadas	Semanal ou mensal, conforme configurado nas preferências do SupportAssist no TechDirect	120 KB
Envio de informações periódicas de monitoramento do PC	A cada 30–45 dias após a implementação	135 KB
Envio de alertas e informações sobre o estado do sistema	Quando um alerta é detectado ou uma falha é observada	145 KB
Criação da solicitação de suporte	Quando um alerta é qualificado para a criação de uma solicitação de suporte	160–350 KB
Verificação de upgrades de versão do SupportAssist	Uma vez por semana	16 KB
Upgrade para a versão mais recente do SupportAssist	Quando a versão mais recente estiver disponível	318 MB
Verificação de recomendações da Dell para atualizações do PC	Duas vezes por semana	1–2 MB*
Verificação de recomendações de atualização inteligente do PC	Duas vezes por semana	65 KB
Envio de insights do PC (informações sobre integridade e experiência no aplicativo)	Uma vez por hora	2.320 KB

Nota: Dados fornecidos com base no SupportAssist for Business PCs versão 3.5.0.
* Os dados variam de acordo com a atualização.



As medidas de segurança físicas e lógicas mantêm os dados armazenados seguros

O que o SupportAssist faz com os dados?

O SupportAssist usa os dados coletados para fornecer suporte automatizado, proativo e preditivo aos clientes. Se houver um problema em um sistema, o SupportAssist vai gerar um alerta para um agente de suporte técnico solucionar.

O SupportAssist também usa dados coletados para prever quando um componente está prestes a falhar, utilizando um software de inteligência artificial com base em dados coletados de dezenas de milhões de sistemas Dell em campo. Esse alerta preditivo pode ser usado para despachar uma peça antes que ela falhe, resultando em tempo de funcionamento ideal do sistema e em proteção de dados.

Por fim, o SupportAssist usa os dados para detectar e remover vírus e malware dos sistemas do usuário, otimizar o desempenho do sistema operacional e dar recomendações sobre atualizações de BIOS, driver e firmware.

O uso de aplicativos do sistema fornece insights sobre o uso do sistema com o componente Insights.

Segurança física

A Dell Technologies Services hospeda os dados do SupportAssist, incluindo aplicativo, sistemas, rede e componentes de segurança, em um data center nos Estados Unidos projetado para manter altos níveis de disponibilidade e segurança. Os dados do SupportAssist são protegidos usando diversas medidas.

O acesso aos data centers em que a infraestrutura reside está restrito a pessoas autorizadas. O acesso é controlado via Smart Card.

Segurança lógica

Os dados gerados pelo SupportAssist 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 restringido por ferramentas internas que são auditadas e avaliadas conforme as diretrizes da Dell Digital (TI).

- **Auditoria:** Os logs de dispositivos monitorados são mantidos, com acesso apenas para os aplicativos e/ou a infraestrutura da Dell Technologies Services. Esses logs registram todas as tentativas de log-in ou acesso ao sistema operacional ou ao console do servidor da Web do SupportAssist.

As compilações gerenciadas por TI são reforçadas usando os controles do Center for Internet Security (CIS) indicados pelas práticas recomendadas de segurança.

Por fim, o ecossistema do SupportAssist emprega a alta disponibilidade local dentro do data center e a infraestrutura idêntica em um data center diferente. 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 aproveita ambientes de nuvem que controlamos e gerenciamos por completo, incluindo nuvens privadas, híbridas e públicas. Bancos de dados relacionais, serviços de armazenamento simples e data warehouses são todos criptografados e usam privilégios mínimos. Nenhum banco de dados relacional é voltado para o público. Os data warehouses são protegidos usando HTTPS.

Quais são as práticas e as políticas de segurança da Dell Technologies?

Desenvolvimento

Nossa norma de ciclo de vida do desenvolvimento seguro (SDL) interna serve como uma referência fundamental para as organizações de produtos da Dell Technologies, fornecendo referências de desempenho essenciais para o desenvolvimento seguro de produtos e aplicativos. A Dell fornece um catálogo de controle do SDL definido com base na ISO/IEC 27034 e uma norma baseada no NIST Secure Software Development Framework (SSDF). Essas ferramentas ajudam as equipes da Dell a criar produtos seguros para os clientes e evitar que vulnerabilidades e deficiências de segurança sejam introduzidas no software e hardware desenvolvidos pela Dell e com suporte dela. A adoção desses controles é obrigatória para equipes de engenharia durante o desenvolvimento de novos recursos e funcionalidades. Esses controles englobam atividades de análise, bem como medidas proativas e prescritivas focadas nas principais áreas de risco.

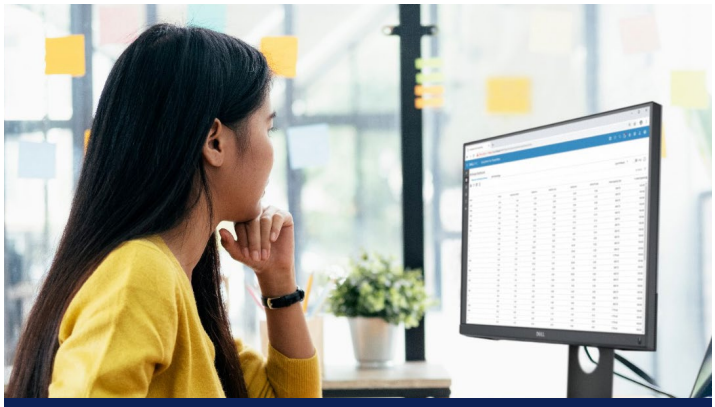
As atividades de análise, incluindo modelagem de ameaças, análise de código estático, varredura e testes de segurança, são componentes integrais destinados a identificar e reduzir defeitos de segurança durante todo o ciclo de vida de desenvolvimento. Além disso, o SDL inclui controles prescritivos para ajudar a garantir que as equipes de desenvolvimento lidem de maneira proativa com questões específicas de segurança, incluindo aquelas descritas nas normas do setor, como o Open Web Application Security Project (OWASP) Top 10 e o SANS Top 25.

O SupportAssist for Business PCs se alinha a essa estrutura eficiente de SDL, empregando o modelo de maturidade do SDL da Dell para implementar controles de segurança de acordo com os padrões do setor. O programa DevSecOps protege os processos modernos de desenvolvimento e implementação de software na Dell automatizando os controles de SDL e impondo políticas de segurança em um ambiente de integração e implementação contínuas (CI/CD). Essas ferramentas de CI/CD automatizam os processos de compilação, teste e implementação, garantindo que as alterações de código sejam integradas e testadas continuamente como parte do fluxo de trabalho de desenvolvimento.

Os engenheiros de SDL realizam avaliações de segurança do SDL para identificar problemas de segurança e vulnerabilidades no software e fornecem recomendações às equipes de desenvolvimento para corrigir essas descobertas de segurança. Essa garantia oferece visibilidade da maturidade das nossas práticas de segurança e da postura de segurança do nosso software e hardware.

A avaliação inclui:

- Avaliação de vulnerabilidade usando testes de penetração.
- Testes de segurança de terceiros realizados por fornecedores respeitados, como a SecureWorks.
- Avaliação de autenticação, autorização e soluções de gerenciamento de identidade.
- Varredura completa de todas as bibliotecas e componentes de terceiros usando ferramentas de análise de composição de software líderes do setor.
- Comunicação dos Aconselhamentos de segurança da Dell para aprimoramentos de segurança específicos.
- Classificação rigorosa de dados em colaboração com nossa organização de segurança global, alinhando os esforços de privacidade e segurança para proteger dados eletrônicos.
- Os aplicativos são submetidos a auditorias de segurança e procedimentos de governança.



Processos seguros e práticas comprovadas do setor mantêm a segurança do SupportAssist.

Teste de validação de segurança

As avaliações de segurança de terceiros são executadas regularmente para o aplicativo SupportAssist e respectiva 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 do Open Web Application Security Project (OWASP), além de bibliotecas de terceiros.

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

Gerenciamento de mudanças

O processo de gerenciamento de mudanças da Dell Technologies segue as práticas recomendadas da ITIL Foundation, conforme determinado pela nossa diretoria corporativa de gerenciamento de mudanças. Todas as mudanças são gerenciadas por tíquetes de solicitação de alteração. Quem acessa nosso sistema para iniciar alterações precisam passar por treinamento da ITIL, bem como familiarização com o SDL. Todas as atualizações e upgrades aplicados à infraestrutura de back-end têm controle de versão para acompanhamento e rastreabilidade adequados. A equipe emprega um processo de compilação automatizado para aplicar novas compilações ou revogar qualquer compilação ou hot fix que tenha sido implementado.

Todas as versões 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 priorizados usando um plano de registro e um processo de gerenciamento de mudanças.

Autenticação

O SupportAssist usa o Dell MyAccount para autenticação na infraestrutura da Dell Technologies Services, chave simétrica aleatória de aplicativos, JWT e grupos de log-in do sistema operacional em autenticação pronta para uso.

Grupos como a equipe de administração do banco de dados e de suporte operacional, que têm acesso aos componentes do SupportAssist, recebem tarefas e direitos de acesso separados. Todas as atualizações no ambiente de produção passam por um processo de controle de mudança definido, que incorpora verificações e balanceamentos.

Comunidade com reconhecimento de segurança

Oferecemos um currículo de treinamento de segurança baseado em funções para instruir funcionários novos e existentes sobre as práticas recomendadas de segurança específicas do trabalho e como usar recursos relevantes. A Dell Technologies se esforça para criar uma cultura de segurança em toda a comunidade. Além disso, nossa comunidade de desenvolvedores faz parte do programa Security Champion da Dell, que foi elaborado para promover Shift Security Left nas práticas de desenvolvimento de software.

Geração de relatórios de incidentes

Na Dell Technologies, todos são obrigados a informar imediatamente à Computer Security Incident Response Team (CSIRT) quaisquer atividades suspeitas, problemas de segurança cibernética ou ameaças pelo e-mail security@dell.com.

Resposta a vulnerabilidades

A Dell Technologies tem o compromisso de minimizar os riscos associados às vulnerabilidades de segurança em nossos produtos, aplicativos e serviços em nuvem. Para alcançar práticas de resposta oportunas às vulnerabilidades, seguimos as diretrizes descritas na Vulnerability Response Standard (VRT) da Dell Technologies. A Dell participa ativamente de vários esforços da comunidade, incluindo o Forum of Incident Response and Security Teams (FIRST) e o Software Assurance Forum for Excellence in Code (SAFECode). Nossos processos e procedimentos estão alinhados com a Estrutura de serviços PSIRT da FIRST, bem como com outras normas, incluindo ISO/IEC 29147:2018 e ISO/IEC 30111:2019.

A Dell Technologies se esforça para resolver as vulnerabilidades em nossos produtos, aplicativos e serviços em nuvem no menor tempo comercialmente razoável. Os cronogramas exatos podem variar dependendo da vulnerabilidade específica e do impacto dela, como a complexidade do esforço/impacto da vulnerabilidade a ser corrigida. Nossa equipe de resposta a incidentes de segurança do produto (PSIRT) coordena a resposta e a divulgação de todas as vulnerabilidades de produtos que nos são informadas. Todas as divulgações de vulnerabilidades de produtos da Dell Technologies são disponibilizadas on-line na página Aconselhamentos, avisos e recursos de segurança da Dell. Para obter mais detalhes sobre as práticas de resposta a vulnerabilidades da Dell, consulte a Política de resposta a vulnerabilidades da Dell.

Líder do setor na definição de práticas recomendadas de segurança dos produtos e no aprimoramento da causa do desenvolvimento seguro.

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 práticas recomendadas de segurança do produto e na melhoria da causa do desenvolvimento seguro. Alguns exemplos de colaboração do setor:

- A Dell Technologies cofundou e atualmente preside a Diretoria do 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 treinamento de garantia de software.

Afiliações do setor (continuação)

- A Dell Technologies é um membro ativo do Forum of Incident Response and Security Teams (FIRST). A FIRST é uma organização de primeira linha e líder global reconhecida em resposta a incidentes e vulnerabilidades.
- Participamos ativamente do Open Group Trusted Technology Forum (OTTF). O OTTF lidera o desenvolvimento de um programa e estrutura global de integridade da cadeia de suprimentos.
- 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.

Normas de segurança do setor

- Os funcionários da Dell estão envolvidos ativamente em órgãos de normas e em consórcios do setor, que se concentram no desenvolvimento de normas de segurança e na definição de práticas de segurança em todo o setor, incluindo:
- Cloud Security Alliance (CSA)
- The Forum of Incident Response and Security Teams (FIRST)
- The Open Group
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

A Dell Technologies tem certificação ISO 9001. Nossa empresa realiza auditorias trimestrais e revisão de conformidade regulares para todos os centros de desenvolvimento e produção.

V. Conclusão

A tecnologia de conectividade SupportAssist oferece recursos inteligentes de automação e correção para viabilizar o tempo máximo de funcionamento do parque de desktops e notebooks Dell de uma organização. A Dell Technologies Services fornece essa tecnologia de ponta com segurança ideal, concentrando-se em processos seguros e na transmissão e armazenamento seguros de dados.

Em caso de dúvidas e para obter mais informações, acesse Dell.com/SupportAssist

[1] Para conhecer os requisitos e sistema compatíveis, consulte nosso Guia do administrador e selecione os PCs compatíveis. Os recursos proativos e preditivos dependem do seu plano de serviço ativo e das regras de negócios da Dell Technologies. Para conhecer os recursos do ProSupport Suite for PCs, consulte nosso Guia do administrador e selecione Conectar e gerenciar recursos e planos de serviço da Dell.

[2] Com base em uma análise da Dell, de dezembro de 2023.