SupportAssist for Business PCs: Visão geral de segurança

Cinco dúvidas importantes que você pode ter sobre a segurança do SupportAssist e as respectivas 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 de utilização e correção do PC com base no plano de serviços.

Conteúdo

I: Introdução

Falhas no notebook causam disrupção e frustração. Esses problemas podem afetar severamente a produtividade do funcionário, 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 PCs.

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. As informações sobre o estado dos sistemas do usuário final são enviadas ao departamento de TI da empresa ou a um fornecedor de hardware ou software para resolver ou evitar problemas rapidamente. 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:

- Que dados o SupportAssist coleta?
- Como esses dados são protegidos à medida que são transmitidos de volta ao departamento de TI da empresa ou ao fornecedor de computadores?
- Após atingir seu destino, esses dados são armazenados de modo que permaneçam privados e seguros?
- Como a Dell segue o RGPD e outras normas?

Este artigo avalia essas e outras questões relacionadas como um meio de avaliar tecnologias habilitadas para ciência de dados. Ele traz uma breve visão geral de como o SupportAssist, como parte do ProSupport Suite for PCs, oferece um serviço de suporte abrangente capaz de prever e resolver problemas antes que eles ocorram. 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 a tecnologia de conectividade inteligente[1] da Dell 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 um problema é detectado, o SupportAssist automaticamente abre um caso com o suporte técnico de acordo com o plano de serviço. O tipo de problema determinará se o alerta iniciará uma solicitação de suporte técnico ou acionará 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 só 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 integridade, experiência de aplicativos e pontuações de segurança em uma única tela
- Biblioteca de scripts criados pela Dell para automatizar tarefas e corrigir problemas em toda a frota
- Automatização do processo de criação e implementação de catálogos personalizados de atualização de BIOS, drivers, firmware e aplicativos da Dell
- Flexibilidade para personalizar suas visualizações 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.

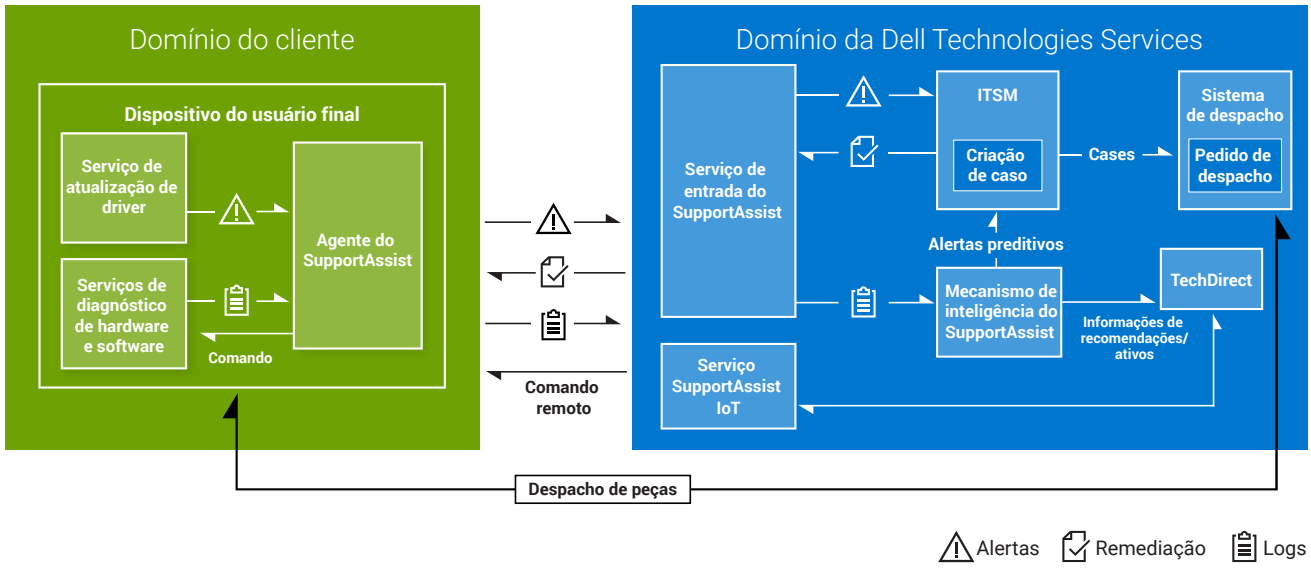
Para obter uma lista completa de recursos e funcionalidades, consulte o Guia do administrador.

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 envio de recomendações.

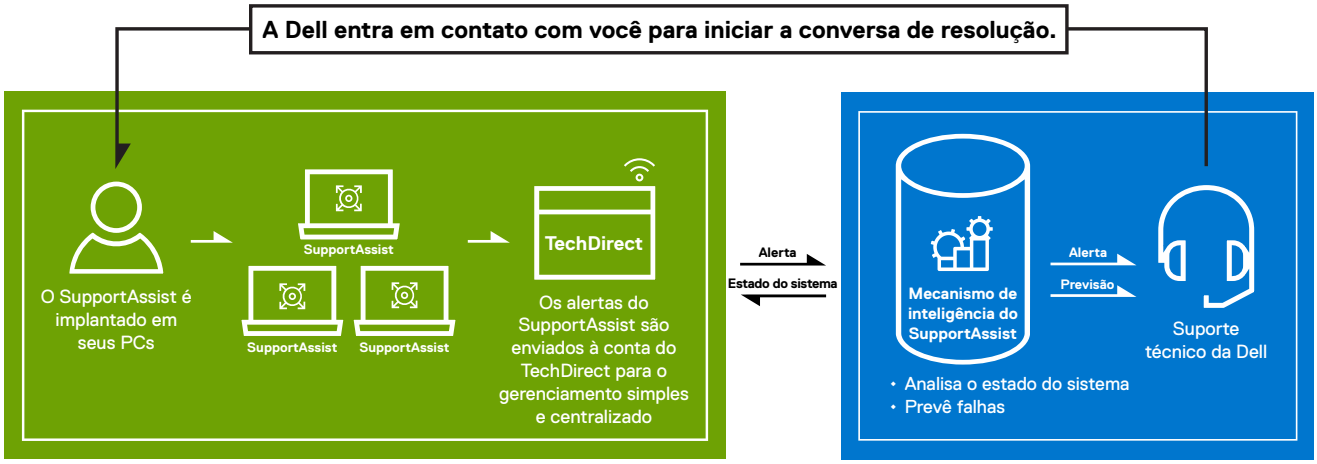
Para obter uma lista completa dos requisitos de rede, endpoint, portas, firewall ou gateway para implementação e correção do SupportAssist, consulte nosso guia de implementação. Nossos scripts de correção foram desenvolvidos pela Dell, testados e assinados e depois confirmados antes da execução.

Arquitetura do SupportAssist



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.

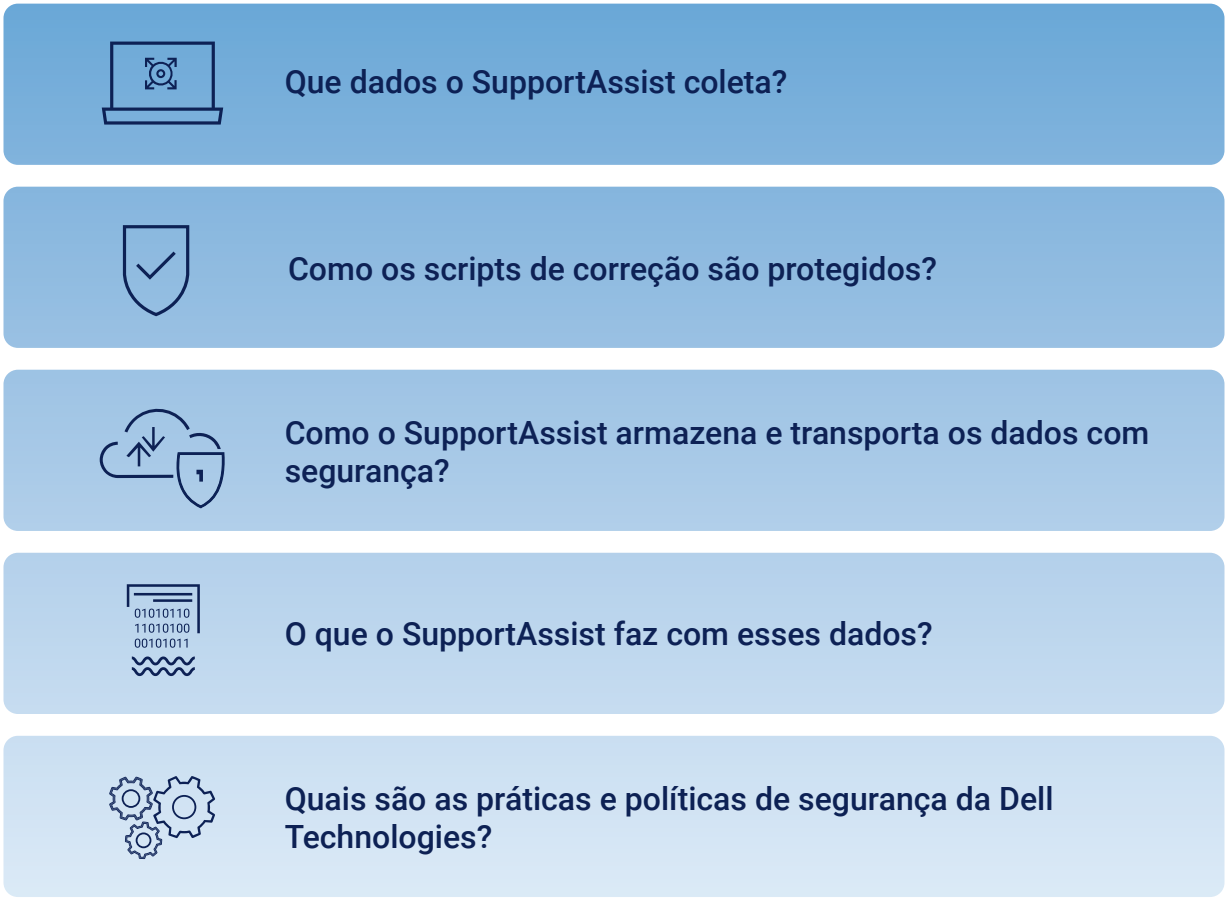


Gerencie o SupportAssist de modo centralizado usando o TechDirect (continuação):

Os insights do SupportAssist, um componente analítico muito útil, coletam dados de utilização do sistema que podem ser visualizados no 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 dúvidas sobre os tipos de dados que o SupportAssist coleta e como esses dados são gerenciados. 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.



Que 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, a Dell usa as informações de contato existentes armazenadas com segurança (criptografia, políticas de retenção etc.) 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 para a Dell Technologies Services
- **Versão do BIOS:** versão do BIOS instalada no sistema
- **Status:** status do alerta, dependendo da gravidade, por exemplo, aviso
- **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 último 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
- **24 horas de contagem de BSOD:** número de ocorrências de tela azul nas últimas 24 horas
- **Informações de 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 os scripts de correção são protegidos?

Antes de serem carregados na plataforma de correção, todos os scripts de correção criados pela Dell são assinados com certificados da Dell e passam por extensos testes e validações para garantir que funcionem conforme o pretendido, sem produzir resultados inesperados. Isso serve como base para verificar a autenticidade do script antes da execução. Por exemplo, se um script for modificado ou substituído no endpoint, a validação da assinatura do certificado falhará e o SupportAssist bloqueará a execução do script. Isso impede a execução de código não autorizado ou potencialmente prejudicial. Esses scripts não podem ser modificados por ninguém fora da Dell, garantindo a integridade. Recomenda-se testar os scripts em um grupo designado de PCs antes de uma implementação mais ampla.

Um processo diferente é seguido para scripts de fluxo de trabalho personalizados. Quando os clientes carregam os próprios scripts, o sistema de correção aceita scripts não assinados e scripts assinados com um certificado do cliente. A integridade desses scripts é preservada durante o trânsito para os PCs e quando armazenados em repouso. Recomenda-se testar os scripts personalizados em um grupo específico de PCs antes de uma implementação mais ampla.

O TechDirect Connect and Manage é compatível com a criação de locais e grupos, permitindo que os clientes validem scripts criados pela Dell e personalizados em máquinas de teste. Todas as informações no console de correção são protegidas dentro dos limites do locatário no TechDirect, acessíveis apenas aos usuários com funções apropriadas atribuídas pelo administrador do locatário. Os resultados também podem ser exportados para um arquivo CSV para análise posterior.

Como o SupportAssist armazena e transporta os dados com segurança?

Os dados enviados do SupportAssist para a Dell Technologies Services são criptografados com a criptografia de 256 bits e 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 client 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. Consulte o documento Dados coletados de PCs conectados para saber mais sobre o consumo médio de dados.

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.

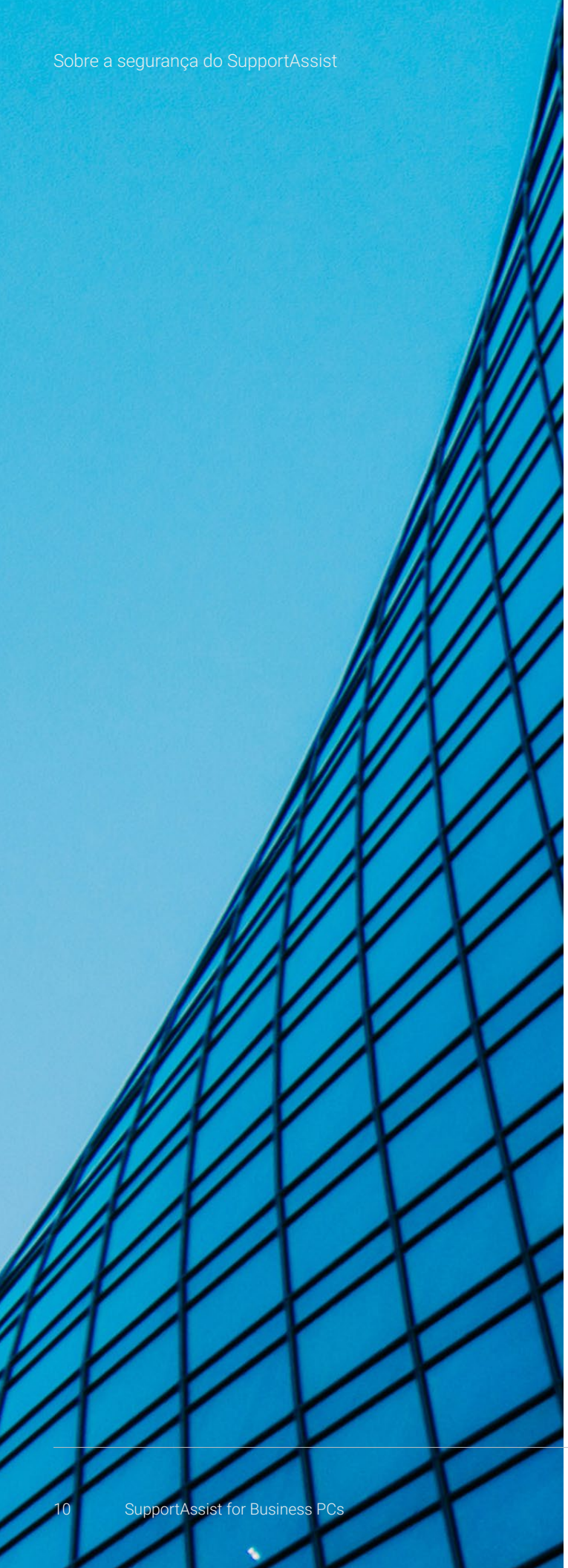
O uso de aplicativos do sistema fornece insights sobre o uso do sistema com o componente Insights.

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.

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



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 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.

RGPD

A Dell implementou medidas projetadas para garantir que tenhamos os processos e procedimentos necessários para cumprir nossas obrigações de acordo com o RGDP. A Dell acompanha desenvolvimentos em leis de privacidade em todo o mundo e garante a conformidade com as obrigações aplicáveis de acordo com a legislação de privacidade relevante. Quando a Dell atua como processadora, ela o faz de acordo com um formulário mutuamente acordado; caso contrário, ela utiliza um formulário padrão de contrato de processamento de dados. Para obter mais informações, acesse estes links:

- Declaração corporativa e resumo dos controles de segurança das informações de RGDP da Dell
- Compromisso da Dell de conformidade com RGPD
- Perguntas frequentes sobre conformidade da Dell para clientes da Dell Technologies

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 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 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 diretoria corporativa de gerenciamento de mudanças. Todas as mudanças são gerenciadas por tíquetes de solicitação de alteração. Quem acessa o sistema para iniciar alterações precisa passar por treinamento da ITIL, bem como se familiarizar 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

A Dell oferece um currículo de treinamento de segurança baseado em funções para instruir funcionários novos e atuais 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, a 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 da vulnerabilidade

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

A Dell Technologies se esforça para resolver as vulnerabilidades em 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. A 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.

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.

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

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.
- A Dell participa 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.

Padrões 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. A Dell realiza auditorias e revisões de conformidade trimestrais regulares para todos os centros de desenvolvimento e fabricação.

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 sistemas compatíveis e requisitos, consulte nosso Guia do usuário (versão do SupportAssist for Home PCs para uso pessoal) ou o Guia do administrador (versão do SupportAssist for Business PCs para gerenciamento de parques de PCs) e clique em "Supported PCs". 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 clique em "Connect and manage capabilities and Dell service plans". Para acessar os recursos do Dell Care Suite, Premium Support Suite ou Alienware Care Suite for PCs, consulte o Guia do usuário e clique em "SupportAssist capabilities and Dell service plans".

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