SupportAssist for Business PCs: 보안 개요

SupportAssist 보안과 관련하여 제기할 수 있는 5가지 주요 질문과 답변

SupportAssist를 사용하면 PC 그룹 전반에서 하드웨어와 소프트웨어 문제를 파악하여 Dell Technologies의 지원을 자동화할 수 있습니다. SupportAssist는 시스템 성능 및 안정화 문제를 해결하고, 보안 위협을 줄이고, 하드웨어 오류를 모니터링 및 탐지하고, Dell 기술 지원 부서와의 협력 프로세스를 자동화합니다.

또한 SupportAssist는 PC에서 텔레메트리 데이터를 사전 예방적으로 수집하고 서비스 계획에 따라 PC 활용도 및 문제 해결에 대한 통찰력을 제공합니다.

목차

I: 소개

노트북에 장애가 발생하면 업무에 지장을 주고 불편을 야기할 수 있습니다. 이러한 문제는 직원의 생산성에 심각한 영향을 미칠 수 있으며 종종 최악의 순간에 발생할 수 있습니다. 이 때문에 기업의 CIO들은 PC 제품의 품질과 가동 시간에 대해 점점 더 우려하고 있습니다.

많은 CIO들이 데이터 사이언스에서 얻은 통찰력을 활용하여 수십억 개의 데이터 포인트를 처리하고 IT 관리자의 효율성을 높이는 최신 첨단 기술로 눈을 돌리고 있습니다. 최종 사용자 시스템의 시스템 상태 정보는 회사의 IT 부서 또는 하드웨어 또는 소프트웨어 공급업체로 전송되어 문제를 신속하게 해결하거나 방지합니다. SupportAssist 연결 기술을 사용하는 Dell ProSupport Plus는 TechDirect 포털에서 전체 PC 그룹을 한눈에 볼 수 있도록 하여 장애가 발생한 하드 드라이브에 대한 알림을 보냅니다.

가동 시간과 효율성을 보장하려면 이 기술이 필요하지만, CIO는 가끔 수집한 정보와 정보 처리 방법에 대해 의문을 제기하기도 합니다.

주요 질문은 다음과 같습니다.

- SupportAssist는 어떤 데이터를 수집합니까?
- 수집한 데이터가 회사의 IT 부서나 컴퓨터 공급업체로 재전송되는 경우 어떤 방식으로 보호됩니까?
- 저장 위치에 도달한 데이터는 비공개 상태로 안전하게 저장됩니까?
- Dell Technologies는 GDPR과 그 밖의 규정을 어떻게 준수합니까?

이 백서는 데이터 사이언스 지원 기술을 평가하는 수단으로 이러한 질문과 기타 관련 질문에 대한 답변을 제시합니다. ProSupport Suite for PCs의 일부인 SupportAssist가 문제가 발생하기 전에 예측하고 해결할 수 있는 포괄적인 지원 서비스를 어떻게 제공하는지에 대한 간략한 개요를 제공합니다. 또한 Dell Technologies Services가 기밀 데이터를 처리, 전송, 저장하는 과정에서 이를 보호하는 방법을 자세히 살펴봅니다.

II: SupportAssist 정보

SupportAssist는 조직이 전체 PC 제품에 대해 자동화된 기술 지원을 받을 수 있도록 지원하는 Dell Technologies의 스마트 연결 기술[1]입니다. 이 서비스는 최종 사용자 디바이스를 모니터링하고, 하드웨어 및 소프트웨어 문제를 사전 예방적으로 탐지하며, 시스템 사용에 대한 통찰력을 제공합니다.

문제가 감지되면 SupportAssist가 서비스 계획에 따라 기술 지원을 통해 자동으로 지원 케이스를 개설합니다. 문제의 유형에 따라 알림을 통해 기술 지원 요청을 시작할지 아니면 자동 부품 디스패치를 작동할지가 결정됩니다. SupportAssist는 기술 지원 부서에서 문제를 해결하는 데 사용하는 하드웨어 및 소프트웨어 데이터를 모두 수집합니다.

Dell ProSupport Suite for PCs는 여러 서비스를 사용할 필요 없이 하나의 솔루션으로 가장 포괄적인 지원 기능을 제공합니다.[2] 자세히 알아보십시오.

주요 기능

- 더 빠른 문제 해결을 위한 전체 디바이스 수준의 사전 예방적이고 예측적인 탐지
- 하나의 화면에서 상태, 애플리케이션 경험 및 보안 점수를 빠르게 분석
- 전체 PC 그룹에서 작업을 자동화하고 문제를 해결하기 위해 Dell이 작성한 스크립트 라이브러리
- Dell BIOS, 드라이버, 펌웨어 및 애플리케이션을 위한 맞춤형 업데이트 카탈로그 생성 및 배포 자동화
- TechDirect에서 뷰와 대시보드를 유연하게 맞춤 구성

사용 가능한 기능은 구매한 PC용 지원 계획에 따라 다릅니다.

- ProSupport Plus를 사용하면 최종 사용자는 예측적 문제 탐지 및 장애 방지를 비롯한 모든 SupportAssist 기능을 활용할 수 있습니다.

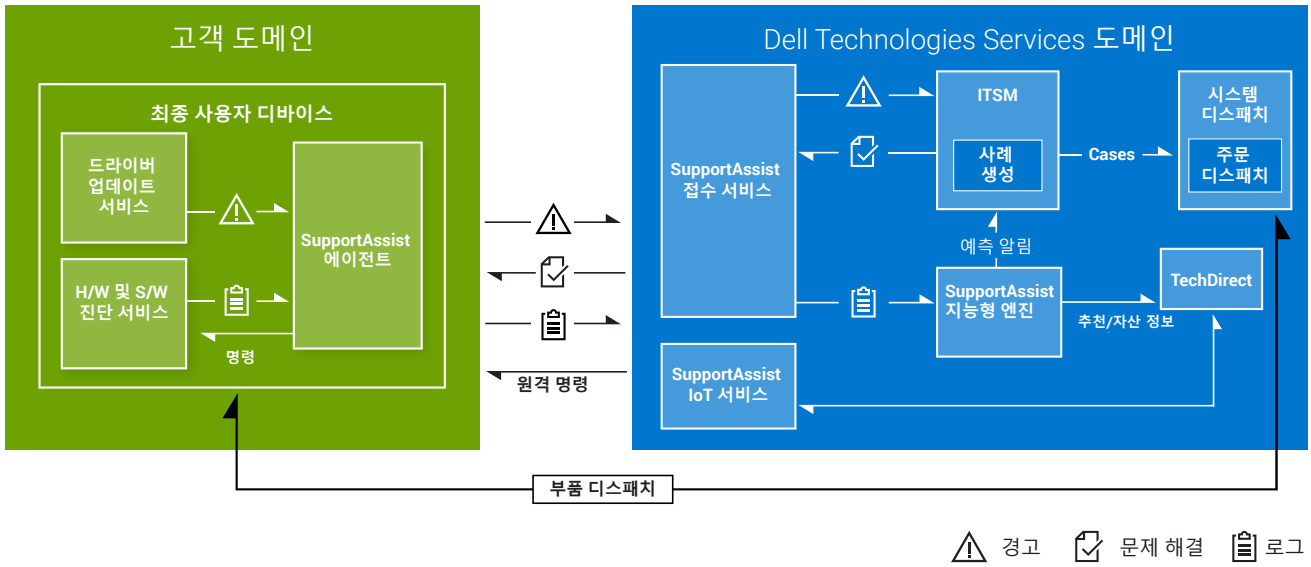
특징과 기능의 전체 목록은 관리자 가이드를 참조하십시오.

III. SupportAssist 아키텍처

SupportAssist는 시스템을 지속적으로 모니터링하고 디바이스에서 일정에 따라 상태 점검을 실행하는 일련의 서비스로 구성됩니다. 이 정보는 Dell Technologies 서버로 다시 전송되어 데이터를 분석하고 권장 사항을 제공합니다.

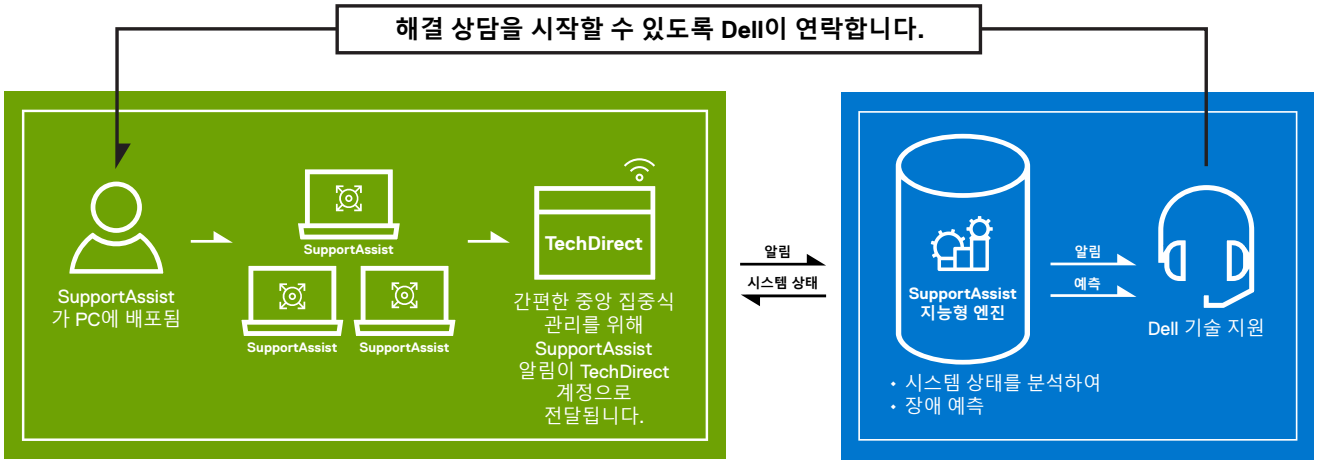
SupportAssist 배포와 문제 해결을 위한 네트워크, 엔드포인트, 포트, 방화벽 또는 게이트웨이 요구 사항의 전체 목록은 배포 가이드를 참조하십시오. 문제 해결 스크립트는 Dell Technologies에서 개발, 테스트 및 서명한 후 실행하기 전에 확인을 거칩니다.

SupportAssist 아키텍처



TechDirect를 사용하여 SupportAssist를 중앙에서 관리

SupportAssist 알림은 간편한 중앙 집중식 관리를 위해 조직의 TechDirect 계정으로 전달될 수 있습니다. ProSupport 또는 ProSupport Plus 서비스 계획을 사용하는 조직은 Dell Technologies Services에 알림을 자동으로 전달할 수도 있습니다.

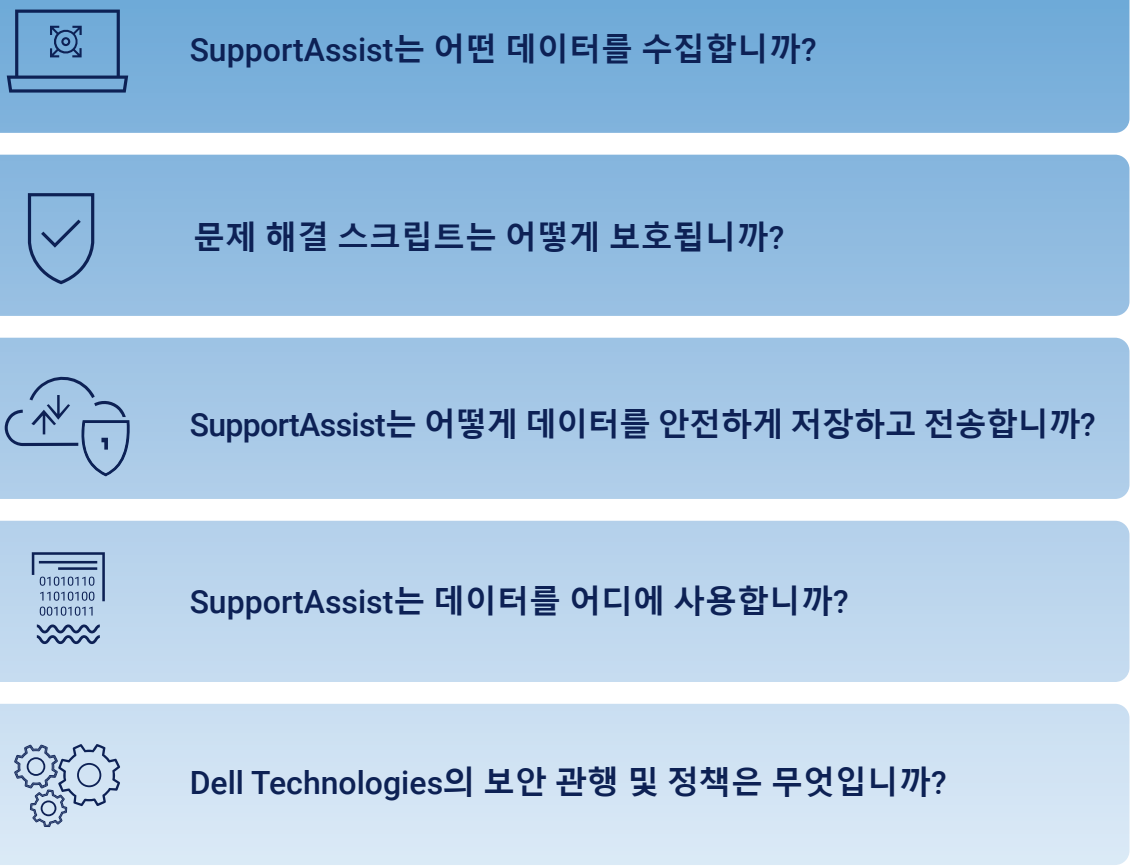


TechDirect를 사용하여 SupportAssist를 중앙에서 관리(계속):

매우 유용한 분석 구성 요소인 SupportAssist Insights는 TechDirect 내에서 볼 수 있는 시스템 활용도 데이터를 수집합니다. 여기에는 CPU 활용도, 사용 가능한 드라이브 공간, 최대 배터리 용량, 배터리 지속 시간 등 많은 유용한 정보가 포함됩니다. TechDirect는 모든 시스템, 특정 디바이스 그룹의 시스템 또는 개별 시스템에 대해 이 정보를 표시할 수 있습니다. 고객은 성능 문제를 파악하고, 하드웨어를 업그레이드하거나 교체해야 하는지 등에 대한 더 나은 비즈니스 의사 결정을 내릴 수 있습니다.

IV. SupportAssist 보안

조직의 CIO 또는 CSO가 SupportAssist에서 수집하는 데이터의 유형과 해당 데이터의 관리 방법에 대해 질문할 수 있습니다. 이 섹션에서는 SupportAssist가 고객의 문제를 해결하는 데 필요한 데이터만 수집한 다음 최적의 보안을 염두에 두고 이 데이터를 처리하는 방법을 보여 줌으로써 이러한 질문에 답변합니다.



SupportAssist는 어떤 데이터를 수집합니까?

SupportAssist는 문제 해결에 필요한 데이터를 자동으로 수집하여 기술 지원 부서에 안전하게 보냅니다. 이 데이터를 통해 적응력이 뛰어나고 지능적이며 빠른 지원 경험을 제공할 수 있습니다.

디바이스에서 수집하는 회사에 대한 정보는 서비스 태그가 유일합니다. 이는 작업 중인 특정 최종 사용자 디바이스를 식별하는 데 필요합니다. SupportAssist가 부품을 사전 예방적으로 배송해야 한다고 판단하는 경우 Dell Technologies 서버에 안전하게 저장된(암호화, 보존 정책 등) 기존 연락처 정보를 사용합니다.

다음 시스템 정보는 일상적인 시스템 모니터링의 일환으로 24시간마다 한 번씩 수집되어 전송됩니다.

- **스키마 버전:** 일상적인 시스템 모니터링에 사용되는 스키마 버전
- **에이전트 버전:** 시스템에 배포된 SupportAssist 버전
- **서비스 태그:** 시스템의 고유 식별자
- **시스템 모델:** 시스템의 모델 이름
- **등록 정보:** SupportAssist의 등록 상태
- **OS 버전:** 디바이스에서 실행 중인 운영 체제 버전
- **SP 버전:** 운영 체제의 서비스 팩
- **UTC 날짜:** 일상적인 시스템 모니터링 정보가 Dell Technologies Services로 전송된 날짜 및 시간
- **BIOS 버전:** 시스템에 설치된 BIOS 버전
- **상태:** 심각도에 따른 알림의 상태(예: 경고)
- **설명:** 시스템 장애 관련 정보(예: 높은 CPU 사용량)
- **하드 드라이브 여유 공간:** 시스템 하드 드라이브에서 사용 가능한 여유 공간
- **메모리 사용량:** 사용된 시스템 메모리의 양
- **CPU 사용량:** 사용된 CPU의 양
- **로컬 날짜:** 시스템의 날짜 및 시간
- **마지막 부팅 날짜:** 시스템을 마지막으로 재시작한 날짜 및 시간
- **Windows 업데이트 실행 날짜:** 시스템에서 Windows가 마지막으로 업데이트된 날짜 및 시간
- **BSOD 수(24시간):** 지난 24시간 동안 블루 스크린이 발생한 횟수
- **알림 정보:** 알림의 고유 식별자

활성 시스템에서 수집되는 시스템 모니터링 데이터에 대한 자세한 내용은 Dell.com의 이 페이지를 참조하십시오.

모든 정보는 보안 채널을 통해 전송됩니다.

문제 해결 스크립트는 어떻게 보호됩니까?

Dell에서 작성한 모든 문제 해결 스크립트는 예상치 못한 결과를 생성하지 않고 의도한 대로 작동하도록, 문제 해결 플랫폼에 업로드되기 전에 Dell 인증서로 서명되고 광범위한 테스트 및 검증을 거칩니다. 이는 실행 전에 스크립트의 신뢰성을 확인하는 기초가 됩니다. 예를 들어 엔드포인트에서 스크립트가 수정되거나 교체되면 인증서 서명 검증이 실패하고 SupportAssist가 스크립트의 실행을 차단합니다. 이렇게 하면 권한이 없거나 잠재적으로 유해한 코드가 실행되지 않습니다. 이러한 스크립트는 Dell 외부의 누구도 수정할 수 없어 무결성을 보장합니다. 광범위한 배포를 수행하기 전에 지정된 PC 그룹에서 스크립트를 테스트하는 것이 좋습니다.

맞춤형 워크플로 스크립트의 경우에는 별도의 처리 과정이 있습니다. 고객이 자체 스크립트를 업로드할 때 문제 해결 시스템은 서명되지 않은 스크립트와 고객 인증서로 서명된 스크립트를 모두 허용합니다. 이러한 스크립트는 PC로 전송될 때나 저장되어 있는 동안 그 무결성이 유지됩니다. 광범위한 배포를 수행하기 전에 특정 PC 그룹에서 맞춤형 스크립트를 테스트하는 것이 좋습니다.

TechDirect Connect 및 관리는 사이트 및 그룹 생성을 지원하므로 고객은 테스트 시스템에서 Dell이 작성한 스크립트와 맞춤형 스크립트를 모두 검증할 수 있습니다. 문제 해결 콘솔 내 모든 정보는 TechDirect에서 테넌트 경계 내에 보안되며, 해당 테넌트 관리자가 할당한 적절한 역할을 가진 사용자만 액세스할 수 있습니다. 추가 분석을 위해 결과를 CSV 파일로 내보낼 수도 있습니다.

SupportAssist는 어떻게 데이터를 안전하게 저장하고 전송합니까?

SupportAssist에서 Dell Technologies Services로 전송되는 데이터는 256비트 암호화로 암호화되고 TLS(Transport Layer Security) 프로토콜을 사용하여 안전하게 전송됩니다.

패키지를 설치하는 동안 각 컴퓨터에서 런타임으로 암호화 키가 생성됩니다. 설치된 정보는 솔트와 함께 암호화 키를 사용하여 암호화됩니다. 저장 상태 데이터는 업계 표준 알고리듬을 사용하여 암호화됩니다.

암호화에서 솔트란 데이터, 비밀번호 또는 비밀번호 문구 "해시"하는 단방향 함수에 입력으로 사용되는 랜덤 데이터입니다. 솔트의 주요 기능은 사전 공격(Dictionary Attack) 또는 이에 상응하는 미리 계산된 레인보우 테이블 공격으로부터 방어하는 것입니다.

모든 암호화 키는 보안 난수 생성기를 사용하여 생성됩니다. 전송 중인 데이터는 HTTPS(Hypertext Transfer Protocol Secure)를 통한 TLS를 사용하여 보호됩니다. 모든 암호화 알고리듬은 업계 표준이며, 저장 상태 데이터도 암호화됩니다.

사용자가 제공한 피드백 전송, 진단 텔레메트리 이벤트, Dell.com 또는 Microsoft Azure IoT 허브에서 복원 프로세스에 사용되는 시스템 정보에 대한 API 쿼리를 위한 오프라인 통신에는 HTTPS가 사용됩니다. 게시/구독 방식에는 보안 MQTT가 사용됩니다.

최종 사용자 디바이스로 콘텐츠를 전송하거나 다운로드할 때 클라이언트와 백엔드 인프라스트럭처 간의 통신을 보호하는 데는 표준 HTTPS가 사용됩니다. 텔레메트리 데이터 전송, Dell.com 또는 Microsoft Azure IoT 허브의 백엔드 API와의 통신, Dell.com에서 검색된 콘텐츠 다운로드를 보호하는 데는 HTTPS 또는 보안 MQTT가 사용됩니다.

모든 네트워크 구성 요소는 방화벽 뒤에 위치하며 네트워크 보안 팀이 관리합니다. 네트워크 트래픽은 엄격하게 제어됩니다. 모든 인바운드 트래픽은 특정 포트를 통해 전송되며 적절한 대상 네트워크 주소로만 전송됩니다. SupportAssist는 Dell Technologies Services 인프라스트럭처에 연결해야 하는 다양한 이벤트에 네트워크 대역폭을 활용합니다. 사용되는 대역폭은 SupportAssist가 모니터링하는 타겟 시스템의 수에 따라 달라질 수 있습니다. 평균 데이터 소비량에 대한 자세한 내용은평균 데이터 소비량에 대한 자세한 내용은 연결된 PC에서 수집된 데이터 문서를 참조하십시오.

SupportAssist는 데이터로 무엇을 합니까?

SupportAssist는 수집된 데이터를 사용하여 고객에게 자동화되고 사전 예방적이며 예측적인 지원을 제공합니다. 시스템에 문제가 있으면 SupportAssist는 기술 지원 에이전트가 문제를 해결하도록 알림을 생성합니다.

또한 SupportAssist는 수집된 데이터를 사용하여 구성 요소에 장애가 발생할 시기를 예측합니다. 이를 위해 수천만 대의 Dell 시스템에서 수집한 데이터를 기반으로 하는 인공 지능 소프트웨어를 사용합니다. 이 예측 알림으로 부품에 장애가 발생하기 전에 부품을 디스패치할 수 있으므로 최적의 시스템 가동 시간과 데이터 보호가 가능합니다.

마지막으로 SupportAssist는 데이터를 사용하여 사용자 시스템에서 바이러스와 멀웨어를 탐지하여 제거하고, 운영 체제 성능을 최적화하고, BIOS, 드라이버 및 펌웨어 업데이트에 대한 권장 사항을 제공합니다.

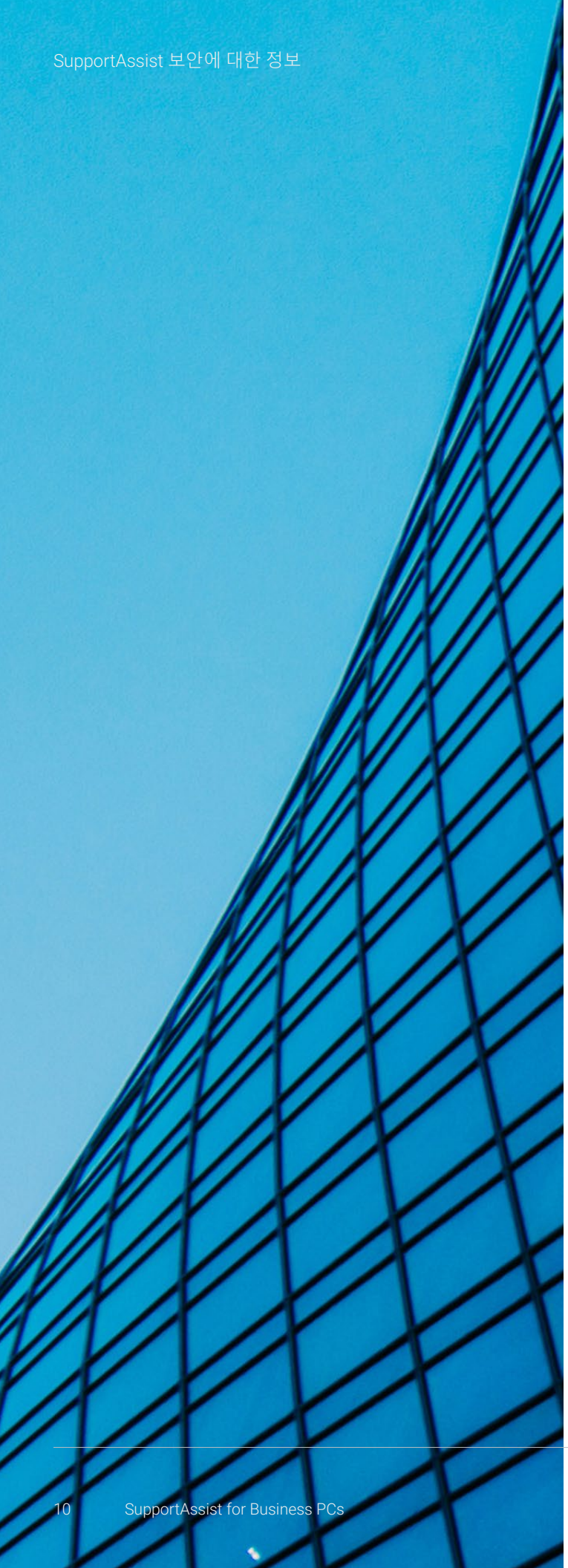
시스템 앱 사용량은 Insights 구성 요소를 통해 시스템 사용량에 대한 통찰력을 제공합니다.

보안 관제

Dell Technologies Services는 SupportAssist 데이터(애플리케이션, 시스템, 네트워크 및 보안 구성 요소 포함)를 높은 수준의 가용성과 보안을 유지할 수 있도록 설계된 미국에 있는 Dell 데이터 센터에서 호스팅합니다. SupportAssist 데이터는 다양한 수단을 사용하여 보호됩니다.

인프라스트럭처가 있는 데이터 센터에 대한 액세스는 허가된 인력으로만 제한됩니다. 액세스는 스마트 카드를 통해 통제됩니다.

물리적 보안 조치와 논리적 보안 조치를 통해 저장된 데이터를 안전하게 유지합니다.



논리적 보안

SupportAssist에 의해 생성된 데이터는 Dell 개인정보 처리방침에 따라 저장됩니다.

Dell Technologies Services 인프라스트럭처(서버, 로드 밸런서, 네트워크 공유 등)에 대한 논리적 액세스는 Dell Digital(IT) 지침에 따라 감사 및 평가되는 내부 툴을 통해 제한됩니다.

- **감사:** 모니터링되는 디바이스 로그는 Dell Technologies Services 인프라스트럭처 및/또는 애플리케이션을 통해서만 액세스할 수 있습니다. 이러한 로그는 운영 체제 또는 SupportAssist 웹 서버 콘솔에 로그인하거나 액세스하는 모든 시도를 기록합니다.

IT 관리 빌드는 보안 모범 사례에 따라 CIS(Center for Internet Security) 권장 제어를 사용하여 강화됩니다.

마지막으로, SupportAssist 생태계는 데이터 센터 내의 로컬 고가용성과 별도의 데이터 센터 내의 동일한 인프라스트럭처를 모두 사용합니다. 유일한 예외는 빅데이터 클러스터 및 프라이빗 클라우드와 같이 본질적으로 고가용성인 기술입니다.

Dell Technologies Services는 데이터 분석을 위해 프라이빗, 하이브리드, 퍼블릭 클라우드를 포함하여 Dell Technologies가 완벽하게 제어하고 관리하는 클라우드 환경을 활용합니다. 관계형 데이터베이스, 단순 스토리지 서비스 및 데이터 웨어하우스는 모두 암호화되며 최소한의 권한만 사용합니다. 관계형 데이터베이스는 공개되지 않습니다. 데이터 웨어하우스는 HTTPS를 사용하여 보호됩니다.

Dell Technologies의 보안 관행 및 정책은 무엇입니까?

개발

Dell Technologies의 내부 SDL(Secure Development Lifecycle Standard)은 제품 조직을 위한 기본 참조 역할을 하며 보안 제품 및 애플리케이션 개발을 위한 필수 벤치마크를 제공합니다. Dell은 ISO/IEC 27034에 따라 정의된 SDL 제어 카탈로그와 NIST SSDF(Secure Software Development Framework)에 기반한 표준을 제공합니다. 이러한 툴은 Dell 팀이 고객을 위한 안전한 제품을 제작하고 Dell에서 개발/지원하는 소프트웨어 및 하드웨어에 보안 취약성과 약점이 생기는 것을 방지하는 데 도움이 됩니다. 이러한 통제는 엔지니어링 팀이 새로운 기능을 개발하는 동안 의무적으로 적용됩니다. 이러한 통제에는 분석 활동뿐만 아니라 주요 위험 영역에 초점을 맞춘 규범적, 사전 예방적 조치도 포함됩니다.

위협 모델링, 정적 코드 분석, 스캔, 보안 테스트를 포함한 분석 활동은 개발 수명주기 동안 보안 결함을 파악하고 완화하는 것을 목표로 하는 필수 구성 요소입니다. 또한 SDL에는 개발 팀이 OWASP(Open Web Application Security Project) Top 10 및 SANS Top 25와 같은 업계 표준에 나열된 문제를 포함하여 특정 보안 문제를 사전 예방적으로 해결할 수 있도록 하는 규범적 통제가 포함되어 있습니다.

SupportAssist for Business PCs는 이 엄격한 SDL 프레임워크를 준수하며, Dell SDL 성숙도 모델을 사용하여 업계 표준에 부합하는 보안 통제 방식을 이행합니다. DevSecOps 프로그램은 CI/CD(Continuous Integration and Continuous Deployment) 환경에서 SDL 제어를 자동화하고 보안 정책을 적용하여 Dell의 최신 소프트웨어 개발 및 배포 프로세스를 보호합니다. 이러한 CI/CD 툴은 빌드, 테스트 및 배포 프로세스를 자동화하여 코드 변경 사항이 개발 워크플로의 일부로 계속해서 통합되고 테스트되도록 합니다.

SDL 엔지니어는 SDL 보안 평가를 수행하여 소프트웨어의 보안 문제와 취약성을 파악하고 개발 팀에 이러한 보안 결과를 수정할 수 있는 권장 사항을 제공합니다. 이러한 보증을 통해 보안 관행의 성숙도와 소프트웨어 및 하드웨어의 보안 태세를 파악할 수 있습니다.

이 평가에는 다음이 포함됩니다.

- 침투 테스트를 통한 취약성 평가.
- SecureWorks와 같은 평판이 높은 공급업체에서 수행하는 타사 보안 테스트.
- 인증, 권한 부여 및 ID 관리 솔루션의 평가.
- 업계를 선도하는 소프트웨어 구성 분석 툴을 사용한 모든 타사 라이브러리 및 구성 요소에 대한 철저한 스캔.
- 특정 보안 개선을 위한 Dell 보안 권고 사항 전달.
- 전자 데이터 보호를 위한 개인 정보 보호 및 보안 활동 기준에 따라 글로벌 보안 조직과 협력하여 엄격한 데이터 분류 실시.
- 애플리케이션에 보안 감사 및 거버넌스 절차 적용.

GDPR

Dell Technologies는 GDPR에 따른 의무를 준수하는 데 필요한 프로세스와 절차를 갖출 수 있도록 고안된 조치를 시행했습니다. Dell은 전 세계의 개인 정보 보호법 개발을 모니터링하고 해당 법령에 따라 적용되는 의무를 준수하여 개인 정보 보호를 강조합니다. Dell이 프로세서 역할을 하는 경우 상호 합의된 양식 또는 표준 데이터 처리 계약 양식에 따라 처리합니다. 자세한 내용은 다음 링크를 참조하십시오.

- Dell Technologies의 GDPR 정보보안 CORPORATE STATEMENT 및 CONTROL SUMMARY
- GDPR 규정 준수에 대한 Dell Technologies의 약속
- Dell Technologies 고객을 위한 Dell 규정 준수 FAQ

보안 프로세스와 검증된 업계 관행을 통해 SupportAssist의 보안을 유지합니다.

보안 검증 테스트

타사 보안 평가가 SupportAssist 애플리케이션과 해당 지원 인프라스트럭처에 대해 정기적으로 수행됩니다.

애플리케이션 평가에는 데이터 전송 및 API 보안, 정적 및 동적 소스 코드 분석, OWASP(Open Web Application Security Project) 교차 점검, 타사 라이브러리가 포함됩니다.

인프라스트럭처 평가에는 내부 및 외부 네트워크 디바이스, 서버 및 서비스 공급업체가 포함됩니다.

변경 관리

Dell Technologies 변경 관리 프로세스는 기업 변경 관리 위원회의 지침에 따라 ITIL Foundation 모범 사례를 따릅니다. 모든 변경 사항은 변경 요청 티켓을 통해 관리됩니다. 변경을 시작하기 위해 시스템에 액세스하는 사람들은 ITIL 교육을 이수하고 SDL을 숙지해야 합니다. 백엔드 인프라스트럭처에 적용되는 모든 업데이트와 업그레이드는 적절한 추적을 위해 버전이 제어됩니다. 팀은 자동화된 빌드 프로세스를 사용하여 새 빌드를 적용하거나 배포된 빌드 또는 핫픽스를 해제합니다.

Dell.com/support로 승격된 모든 릴리스에는 알려진 제한이 적용된 변경 사항에 대한 정보가 포함되어 있습니다.

모든 새로운 기능과 변경 사항은 제품 관리 팀에서 관리하며, 기록 계획 및 변경 관리 프로세스를 사용하여 우선순위를 지정합니다.

인증

SupportAssist는 Dell Technologies Services 인프라스트럭처, 애플리케이션 랜덤 대칭 키, JWT, 기본 인증을 위한 OS 로그인 그룹을 사용한 인증에 Dell MyAccount를 사용합니다.

SupportAssist 구성 요소에 액세스할 수 있는 데이터베이스 관리 팀과 운영 지원 팀 등의 그룹에는 별도의 작업 및 액세스 권한이 할당됩니다. 업무 환경에 대한 모든 업데이트는 견제와 균형을 통합한 정의된 변경 제어 프로세스를 거칩니다.

보안 인식 제고 커뮤니티

Dell Technologies는 직무 기반 보안 교육 과정을 통해 신입 직원과 기존 직원에게 직무별 보안 모범 사례와 관련 리소스 사용 방법을 교육합니다. Dell Technologies는 커뮤니티 전체의 보안 의식을 높이기 위해 최선을 다하고 있습니다. 또한 Dell Technologies의 개발자 커뮤니티는 소프트웨어 개발 관행에서 보안을 초기에 고려하도록 설계된 Dell Technologies의 Security Champion 프로그램에 참여하고 있습니다.

인시던트 보고

Dell Technologies의 모든 직원은 의심스러운 활동, 사이버 보안 문제 또는 위협이 발견되면 security@dell.com에 이메일을 보내 CSIRT(Computer Security Incident Response Team)에 즉시 보고해야 합니다.

취약성 대응

Dell Technologies는 제품, 애플리케이션 및 클라우드 서비스의 보안 취약성과 관련된 위험을 최소화하기 위해 최선을 다하고 있습니다. Dell Technologies는 시기적절한 취약성 대응 관행을 달성하기 위해 Dell Technologies VRT(Vulnerability Response Standard) 표준에 명시된 가이드를 준수합니다. Dell Technologies는 FIRST(Forum of Incident Response and Response Team) 및 SAFECode(Software Assurance Forum for Excellence in Code)를 비롯한 다양한 커뮤니티 활동에 적극적으로 참여하고 있습니다. Dell Technologies의 프로세스와 절차는 FIRST PSIRT 서비스 프레임워크뿐만 아니라 ISO/IEC 29147:2018 및 ISO/IEC 30111:2019를 포함한 기타 표준에도 부합합니다.

Dell Technologies는 합당한 최단 시간 내에 제품, 애플리케이션 및 클라우드 서비스의 취약성을 해결하기 위해 노력하고 있습니다. 정확한 일정은 특정 취약성과 그에 따른 영향, 즉 취약성 해결을 위한 활동과 문제 해결의 영향이 가진 복잡성 등에 따라 달라질 수 있습니다. PSIRT(Product Security Incident Response Team)가 Dell Technologies에 보고된 모든 제품 취약성에 대한 대응과 공개를 조정합니다. Dell Technologies 제품에 대해 공개된 모든 취약성은 Dell Security Advisor, 통지 및 리소스 페이지에서 온라인으로 확인할 수 있습니다. Dell Technologies의 취약성 대응 관행에 대한 자세한 내용은 Dell의 취약성 대응 정책을 참조하십시오.

업계 제휴

Dell Technologies는 업계 차원의 다양한 그룹에 참여하여 선도적인 여러 공급업체와 협력해 제품 보안에 대한 모범 사례를 정의하고 발전시키고 공유하고, 나아가 안전한 개발을 촉진합니다. 업계 협업의 예는 다음과 같습니다.

- Dell Technologies는 SAFECode(Software Assurance Forum for Excellence in Code)를 공동 설립했으며 현재 이사회 의장을 맡고 있습니다. 다른 이사회 구성원으로는 Microsoft, Adobe, SAP, 인텔, Siemens, CA 및 Symantec의 대표자들이 있습니다. SAFECode 구성원은 소프트웨어 보증 관행 및 교육을 공유하고 게시합니다.

제품 보안 모범 사례를 정의하고 보안 개발의 원인을 개선하는 업계 리더.

업계 제휴(계속)

- Dell Technologies는 FIRST(Forum of Incident Response and Security Teams)의 정회원으로 활발하게 활동하고 있습니다. FIRST는 인시던트 및 취약성 대응 분야에서 선도적인 조직이자 인정받는 글로벌 리더입니다.
- Dell Technologies는 OTTF(Open Group Trusted Technology Forum)에 적극적으로 참여하고 있습니다. OTTF는 글로벌 공급망 무결성 프로그램 및 프레임워크의 개발을 주도합니다.
- Dell 직원들은 IEEE 사이버 보안 이니셔티브에 따라 소프트웨어 설계자가 보안 설계 결함을 이해하고 해결할 수 있도록 지원하기 위해 출범한 IEEE Center for Secure Design의 창립 멤버였습니다.

업계 보안 표준

- Dell 직원은 보안 표준을 개발하고 업계 차원의 보안 관행을 정의하는 데 중점을 두는 다음과 같은 업계 컨소시엄에 적극적으로 관여합니다.
- CSA(Cloud Security Alliance)
- FIRST(Forum of Incident Response and Security Teams)
- Open Group
- SAFECode(Software Assurance Forum for Excellence in Code)
- SNIA(Storage Networking Industry Association)

Dell Technologies는 ISO 9001 인증을 받았습니다. Dell Technologies는 모든 개발 및 제조 센터에 대해 정기적인 분기별 감사 및 규정 준수 검토를 실시합니다.

V. 결론

SupportAssist 연결 기술은 지능형 자동화와 문제 해결 기능을 제공하여 조직의 모든 Dell 데스크탑 및 노트북 컴퓨터 그룹의 가동 시간을 극대화합니다. Dell Technologies Services는 보안 프로세스, 보안 데이터 전송 및 보안 데이터 스토리지에 중점을 두고 이러한 첨단 기술을 최적의 보안으로 제공할 수 있습니다.

질문이 있거나 자세한 정보를 보려면 **Dell.com/SupportAssist**를 방문하십시오.

[1] 지원되는 시스템 및 요구 사항은 사용자 가이드(개인용 SupportAssist for Home PCs 버전) 또는 관리자 가이드(PC 그룹 관리용 SupportAssist for Business PCs 버전)를 참조하여 "지원되는 PC"를 클릭하십시오. 사전 예방적이고 예측적인 기능은 현재 진행 중인 서비스 계획과 Dell Technologies 비즈니스 규정에 따라 달라집니다. ProSupport Suite for PCs 기능을 알아보려면 관리자 가이드를 참조하고 "연결 및 관리 기능과 Dell 서비스 계획"을 클릭하십시오. Dell Care Suite, Premium Support Suite 또는 Alienware Care Suite for PCs 기능에 대해서는 사용자 가이드를 참조하고 "SupportAssist 기능 및 Dell 서비스 계획"을 클릭하십시오.

[2] Dell 분석 기준, 2023년 12월.