보안 연결 게이트웨이

Dell Technologies의 기술로 데이터 보호 및 위협 방지를 안전하고 자동화된 지원 환경에 통합

최대

60%

Forrester의 설문조사에서 위험을 줄이는 데 연결 기술을 활용한다고 응답한 IT 리더의 비율[1]

보안 연결 게이트웨이는 PowerEdge 서버용 OpenManage Enterprise 내의 일부 Dell EMC 하드웨어와 특정 서비스 플러그인에 대한 직접 연결 버전으로도 구현됩니다. Dell Technologies Services는 시장, 규정 및 고객 정보를 기반으로 당사의 제품이 고객의 보안 목표 및 규정 준수 요건을 충족하는 데 도움이 되는 보안 기능을 구현하기 위해 최선을 다하고 있습니다.

목차

1: 소개:

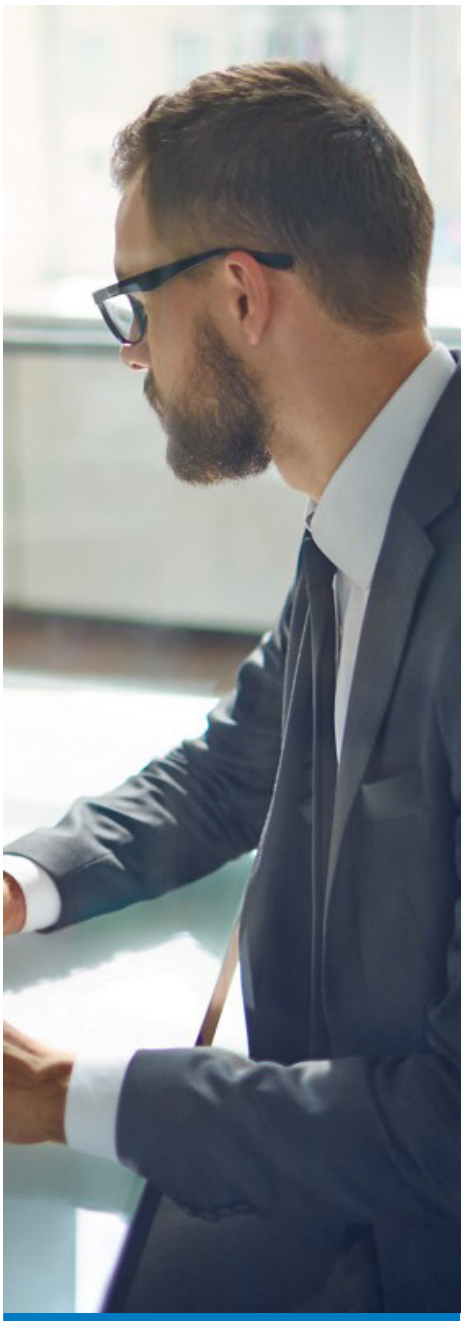
오늘날의 하이퍼 디지털 환경에서 성공적인 혁신 리더는 IT 서비스 공급업체에 IT 지원을 아웃소싱합니다. Dell Technologies Services의 의뢰로 Forrester Consulting에서 실시한 연구[1]에 따르면, IT 리더의 59%가 적합한 IT 서비스 공급업체와의 협력을 통해 IT 직원이 일상적인 업무에서 벗어나 혁신과 전략적 이니셔티브에 할애할 수 있을 것이라고 말합니다.

선도적인 IT 서비스 공급업체인 Dell Technologies Services는 IT 지원 서비스와 기술이 보안 위협의 잠재적인 원인이 되지 않도록 보장합니다. Dell Technologies Services는 고객 환경에 구축된 Dell EMC 제품을 통해 고객 위험을 최소화할 수 있도록 모든 노력을 기울입니다. 이 백서에서는 복잡한 데이터 센터 인프라스트럭처에 맞는 안전하고 자동화된 IT 지원 환경을 제공할 수 있도록 보안 연결 게이트웨이의 설계, 구현 및 운영에 보안 기능이 어떤 방식으로 내장되어 있는지 설명합니다.

지난 25년간 IT 지원 기술을 선도해오고 있는 보안 연결 게이트웨이 보안 아키텍처는 침해 위협을 차단하고 데이터 무결성을 보호할 수 있도록 설계되었습니다. 당사 기술이 문제 파악을 위해 고객의 디바이스를 지속적으로 모니터링하고 신속하게 문제를 해결하는 동안 Dell Technologies Services는 다음을 수행합니다.

- 실행 중인 시스템에서 텔레메트리 및 이벤트 데이터만 활용합니다.
- HTTPS를 사용하여 인터넷을 통해 전송하도록 TLS(Transport Layer Security) 프로토콜을 사용하여 시스템 상태 데이터를 암호화합니다.
- 공인 기술 지원 엔지니어가 다단계 인증을 사용하여 연결된 시스템에 원격으로 액세스하고 문제를 해결합니다.
- 업계를 선도하는 보안 관행을 활용하여 텔레메트리 및 이벤트 데이터를 Dell Technologies Services 내부에서 처리, 저장 및 사용합니다.

또한 Secureworks와 같은 업계 최고의 여러 공급업체를 이용해 보안 연결 게이트웨이 아키텍처와 프로세스 전반에서 통합된 보안 조치를 철저히 검토하여 위험에 노출되지 않고 안전한 경험을 보장합니다.



사이버 공격과 데이터 부정 행위 또는 도난은 CEO의 상위 10가지 우려 사항에 해당합니다.[2]

2: 보안 연결 게이트웨이 정보

Dell Technologies의 보안 연결 기술을 사용하면 시행착오 없이 문제를 예방하고 가장 중요한 프로젝트에 시간을 더 할애할 수 있습니다. 가상 어플라이언스 및 애플리케이션 에디션은 고객 환경과 Dell Technologies Services 간의 안전한 양방향 연결을 제공하므로 데이터 스토리지, 서버, 네트워킹, CI/HCI, 데이터 보호를 비롯하여 데이터 센터 전반에서 Dell EMC 디바이스를 한 곳에서 모니터링하는 데 적합합니다.

또한 PowerEdge 서버용 OpenManage Enterprise 내의 특정 서비스 플러그인과 일부 Dell EMC 제품에 대한 직접 연결 버전으로 당사의 기술을 배포할 수 있습니다. 특정 Dell EMC 하드웨어 및 소프트웨어에 대해 지원되는 연결 옵션을 확인하려면 Dell.com/Support를 방문해 주십시오.

데이터는 보안 연결 게이트웨이의 원동력입니다. Dell Technologies는 고객 환경의 시스템 상태 데이터를 활용하여 현장 및 기술 지원 팀과 구성 요소 제조업체의 수년간 축적된 인시던트 데이터 및 엔지니어링 데이터와의 연관성을 파악합니다.

수집된 시스템 상태 정보에 대한 자세한 내용은 보안 연결 게이트웨이의 보고 가능 항목 및 OpenManage Enterprise용 서비스 플러그인을 참조하십시오.

Dell Technologies의 연결 기술은 머신 러닝 등의 정교한 AI 모델을 사용하여 패턴을 찾고 적용하여 영향을 미치는 문제를 정확하게 탐지합니다. 이를 통해 하드웨어 및 소프트웨어 문제를 식별하고, 케이스를 생성하고, Dell Technologies의 지원을 바탕으로 비용이 발생하기 전에 문제 해결을 시작합니다. 이 기술은 보안 연결 게이트웨이를 통해 연결된 서버 하드 드라이브 및 백플레인의 장애를 예측합니다. 문제 유형에 따라 알림을 통해 자동 부품 디스패치를 개시할 수도 있습니다.

또한 이 기술은 공인 기술 지원 에이전트가 매니지드 디바이스에 원격으로 액세스하여 문제를 해결할 수 있도록 안전한 양방향 통신을 제공합니다.

연결 보안

타사 보안 평가가 보안 연결 게이트웨이와 해당 지원 인프라스트럭처에 대해 정기적으로 수행됩니다.

애플리케이션 평가에는 데이터 전송 및 API 보안, 정적 및 동적 소스 코드 분석, CVE(Common Vulnerabilities and Exposures), OWASP(Open Web Application Security Project) 교차 점검, 타사 라이브러리 및 제품이 포함됩니다.

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

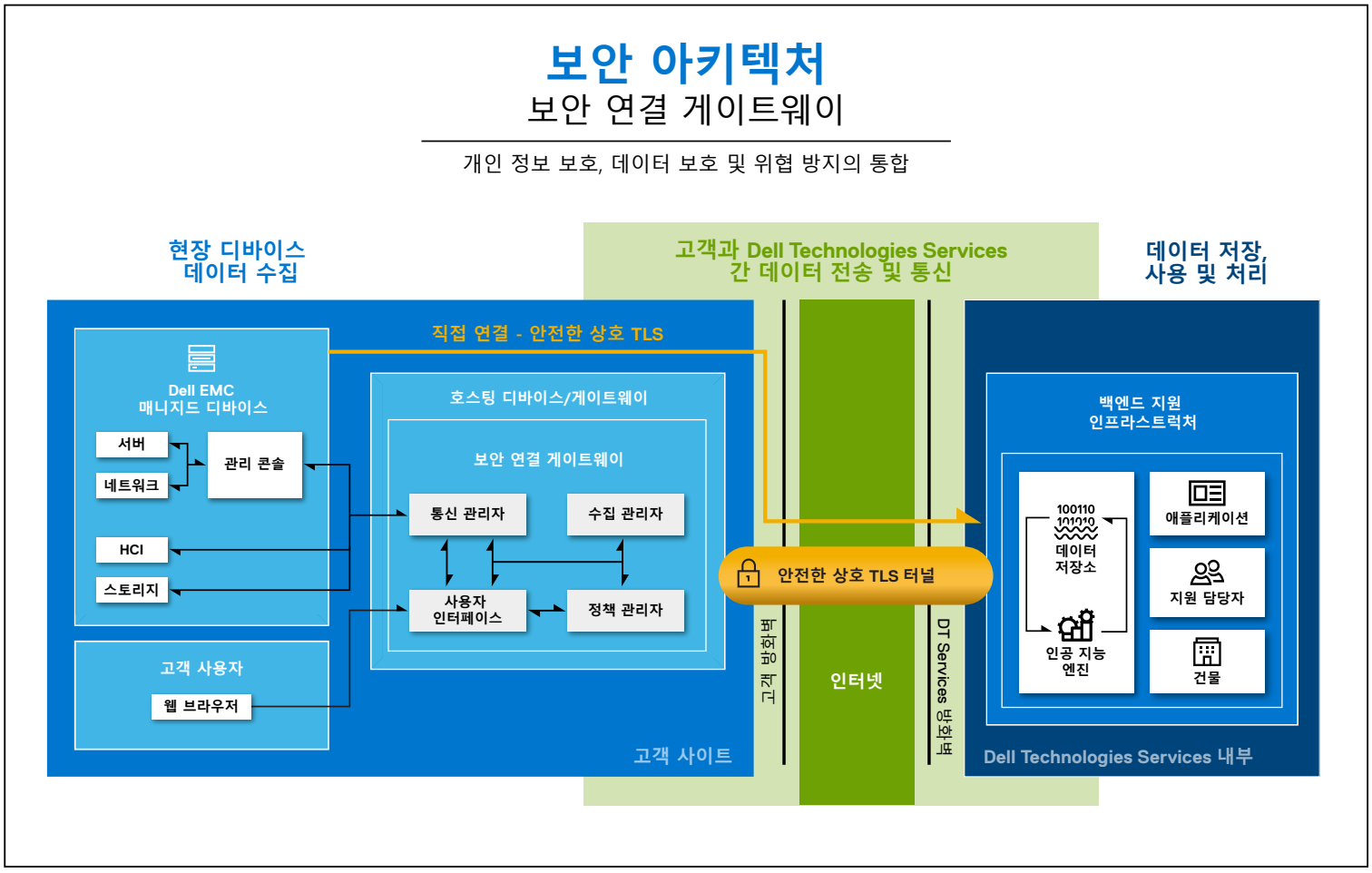
3: 보안 아키텍처 개요

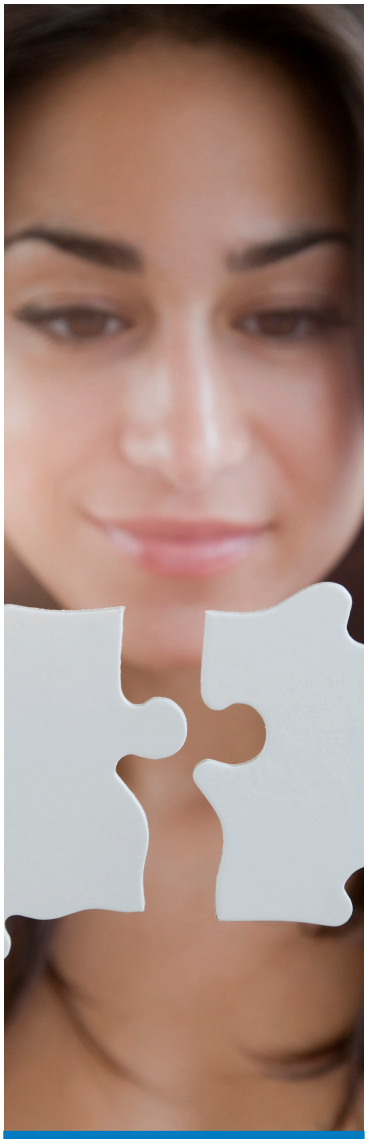
Dell Technologies Services는 자동화된 사전 예방적 및 예측적 연결 기술로 보안 위협에 따른 위험을 최소화하기 위해 최선을 다하고 있습니다. Dell Technologies Services의 보안 아키텍처는 엄격한 업계 표준을 기반으로 구축되며, 제품 개발과 구축의 모든 단계에서 측정 가능하고 반복 가능한 보안 관행을 준수합니다. 자세한 내용은 섹션 4를 참조하십시오.

아래 다이어그램 A는 보안 연결 게이트웨이 보안 아키텍처에 대한 개요를 제공합니다. 다음 섹션에서는 보안 연결 게이트웨이가 Dell 문제를 진단하고 해결하기 위해 필요한 시스템 데이터만 Dell EMC 매니지드 디바이스에서 수집한 다음, 보안과 개인 정보 보호를 최고 수준으로 유지하면서 데이터를 처리하는 방법에 대해 설명합니다.

- 현장 디바이스 데이터 수집
- 데이터 전송 및 통신
- Dell Technologies Services의 데이터 저장, 사용 및 처리

다이어그램 A:





고객은 보안 연결 게이트웨이에서 정책 관리자의 감사 기능을 통해 현장 데이터 수집을 위한 보안 계층을 강화합니다.

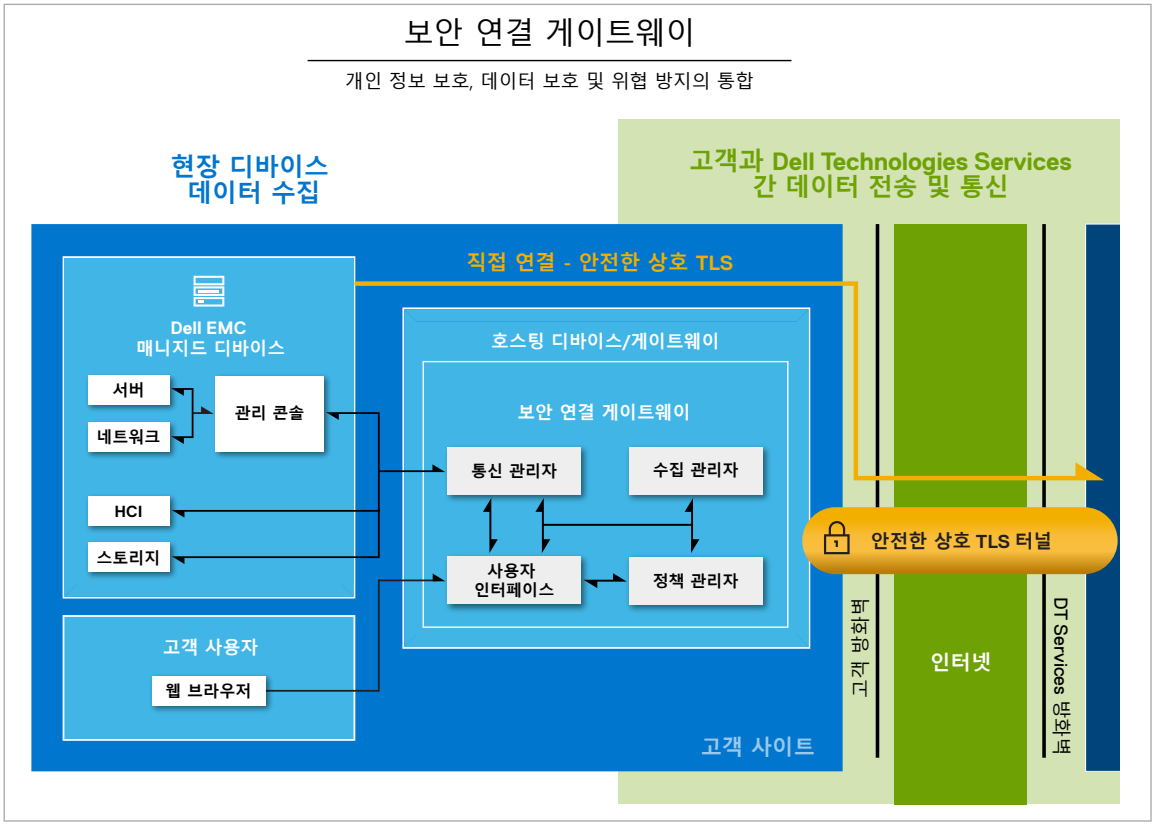
4: 보안 연결 게이트웨이의 상세 보안 접근 방식

4-1: 안전한 현장 데이터 수집

방화벽 액세스 포인트 최소화

보안 연결 게이트웨이는 고객의 방화벽에서 이루어지는 Dell EMC 디바이스 간의 통신을 집계하고 모든 IP 기반 원격 서비스 활동의 단일 진입점 및 진출점 역할을 합니다. 관련 내용은 다이어그램 B를 참조하십시오. Dell Technologies는 원격 IT 지원 기술의 방화벽 액세스 포인트를 최소화하여 회사의 방화벽을 통한 보안 위험을 줄여줍니다.

다이어그램 B(다이어그램 A – 보안 아키텍처에서 발췌):



현장 게이트웨이로서 보안 연결 게이트웨이는 고객이 제공한 하이퍼바이저에 가상으로 배포됩니다. 각 게이트웨이 서버는 매니지드 디바이스 간에 정보를 전달하는 프록시 역할을 합니다. 보안 연결 게이트웨이는 일시적인 로컬 네트워크 장애가 발생하는 경우에도 Connect Home 이벤트를 대기열에 추가할 수 있습니다. 이러한 게이트웨이 서버에는 기본 운영 체제에 기반한 자체 웹 사용자 인터페이스가 있습니다.

일부 고객의 경우, 여러 Dell EMC 하드웨어 제품의 이기종 구축에는 직접 연결 버전이 적합합니다. 이 솔루션은 고객의 방화벽에서 안전한 단일 통신 지점 역할을 합니다. 솔루션이 제품의 운영 환경에 통합되어 있으므로 인바운드 원격 지원 및 Call Home 기능을 제공하기 위한 별도의 서버는 필요하지 않습니다.

방화벽 액세스 포인트 최소화(계속)

OpenManage Enterprise 시스템 관리 콘솔을 사용하는 PowerEdge 데이터 센터의 고객의 경우 내장된 서비스 플러그인을 대체 구현 옵션으로 사용할 수 있습니다. OpenManage Enterprise 가상 어플라이언스 내의 이 연결 플러그인은 고객이 제공한 하이퍼바이저에서 실행되며, 매지니드 서버 및 섀시 디바이스에서 서비스 자동화 계층 역할을 하고 Dell Technologies Services 백엔드에 대한 단일 보안 직접 연결을 제공합니다.

안전한 통신 브로커 역할 수행

보안 연결 게이트웨이는 매니지드 디바이스, 정책 관리자 및 Dell Technologies Services 백엔드 지원 인프라스트럭처 간의 통신 브로커 역할을 합니다. 구축된 게이트웨이 서버는 HTTPS 핸들러로 설정됩니다. 게이트웨이는 디바이스 검색, 이벤트 관리, 텔레메트리 데이터 수집, 텔레메트리 데이터 관리를 비롯한 여러 통신 방식을 활용합니다. 메시지 유형은 다음과 같습니다.

- 디바이스 상태 하트비트 폴링
- 데이터 파일 전송(Connect Home)
- 라이선스 사용량 데이터 전송
- 사용자 인증 요청
- 디바이스 관리 동기화

모든 메시지는 여러 프로토콜을 사용하여 보호됩니다. 다음 섹션에서는 종합적인 TLS(Transport Layer Security) 터널링 및 업계 표준 암호화와 함께 HTTPS 프로토콜을 사용하는 방법을 비롯하여 보안 연결 게이트웨이를 통한 데이터 통신 및 전송 시 기본 제공되는 추가 보안 기능에 대해 자세히 살펴봅니다.

고객의 인증 요건 및 액세스 권한 제어

고객의 데이터 센터에서 보안 연결 게이트웨이를 통해 디바이스를 모니터링하는 경우, 고객은 정책 관리자를 사용하여 원격 액세스 연결, 진단 스크립트 실행 및 기타 관련 활동에 대한 인증 요건을 제어할 수 있습니다. 고객은 직원뿐만 아니라 원격 연결을 통해 문제를 진단하고 해결하는 기술 지원 엔지니어의 액세스 권한도 설정할 수 있습니다.

인증 및 사용 권한 관리에 대한 보안은 다음 정책 관리자 기능을 통해 다음과 같이 보장됩니다.

- 보안 연결 게이트웨이는 정기적으로 정책 관리자를 폴링하여 사용 권한을 변경하고 로컬로 캐싱합니다. 정책 관리자의 경우:
  - 마지막 폴링 주기 이후 구성 업데이트 시 규칙 집합 캐시가 자동으로 업데이트됩니다.
  - 정해진 특정 포트에서 HTTPS 수신기로 메시지를 받도록 구성됩니다.
- 보안 연결 게이트웨이에서 원격 액세스 요청 또는 다른 작업을 수신하면 정책 관리자 캐시에서 수신한 정책이 적용됩니다.
  - 사용 권한은 디바이스 유형 또는 디바이스 유형의 특정 모델에 따른 정책을 사용하여 계층적으로 할당될 수 있습니다.
  - 고객은 정책 관리자의 웹 사용자 인터페이스를 통해 요청된 작업을 수락하거나 거부할 수 있습니다. 또한 필터를 생성하여 인증 및 작업에 대한 추가 제한을 설정할 수 있습니다.

로깅 및 감사 추적

고객은 보안 연결 게이트웨이에서 정책 관리자의 감사 기능을 통해 현장 데이터 수집을 위한 추가 보안 계층을 사용할 수 있습니다. 정책 관리자는 모든 원격 서비스 이벤트 및 연결, 진단 스크립트 실행 및 지원 파일 전송 작업을 기록합니다. 그런 다음 이를 데이터베이스에 플랫 텍스트 감사 로그 파일로 저장하고 정책 관리자, 정책 변경 사항, 모든 액세스 승인 또는 거부 작업에 대한 액세스를 추적합니다.

고객은 다음과 같은 방법으로 모든 정보를 간편하게 확인할 수 있습니다.

- 감사 내용은 정책 관리자 웹 사용자 인터페이스를 통해 볼 수 있으며, 편집할 수는 없습니다.
- 환경 내의 syslog 서버에 스트림하도록 감사 로그를 구성할 수도 있습니다.

보안 연결 게이트웨이

지원되는 TLS 1.2 암호화 그룹:

- 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

디바이스 제어 보안 옵션

고객이 인증 및 사용 권한 관리를 위해 항상 정책 관리자를 사용하도록 설정하는 것은 아니므로, 보안 연결 게이트웨이는 디바이스 제어 옵션을 통해 관련 보안 기능을 제공합니다.

고객은 다음을 수행할 수 있습니다.

- 디바이스 유형, 관리자 그룹, 조직 또는 사업부, 디바이스의 물리적 위치, 선택한 기타 모든 기준을 바탕으로 맞춤형 그룹을 생성합니다.
- 해당 디바이스 그룹에 따라 특정 사용 권한 및 액세스 권한을 정의합니다.

기술 지원 엔지니어의 원격 활동을 비롯한 모든 디바이스 관리 작업이 기록됩니다. 이러한 작업은 기술 지원 에이전트에 의해 백엔드에서도 승인을 받아야 합니다.

이러한 방식으로 고객은 보안 연결 게이트웨이를 통해 관리되는 디바이스에 대한 완벽한 제어 및 투명성을 유지합니다.

2단계 인증 및 디지털 인증서 관리

인증은 안전한 현장 데이터 수집의 중요한 구성 요소입니다. 보안 연결 게이트웨이는 고객 게이트웨이 서버에 배포 시 디지털 인증서를 ID 증명으로 사용합니다. 이 인증서는 게이트웨이 서버의 ID를 백엔드와의 통신을 암호화하고 인증하는 데 사용되는 키 쌍으로 바인딩합니다. Dell Technologies Services의 CA(Certificate Authority)는 보안 연결 게이트웨이 키 인프라스트럭처를 위한 중앙 저장소입니다.

디지털 인증서 관리는 민간 인증 기관에 디지털 인증서 등록을 자동화하는 데 사용됩니다. 이러한 방법을 통해 다음을 수행할 수 있습니다.

- 각 인증서 요청을 프로그래밍 방식으로 생성하고 인증할 수 있습니다.
- 인증서를 게이트웨이 서버를 대상으로만 발급하고 설치할 수 있습니다. 다른 머신에서는 이 인증서를 복사하여 사용할 수 없습니다.

보안 연결 게이트웨이는 백엔드 지원 인프라스트럭처에 배포된 디지털 인증서를 사용하여 연결하고 인증합니다. 기술 지원 에이전트는 2단계 인증을 사용하여 고객 환경의 보안 연결 게이트웨이에 연결합니다.

4-2: 안전한 데이터 전송 및 통신

안전한 통신 터널

고객과 Dell Technologies Services 백엔드 지원 인프라스트럭처 간의 모든 통신은 고객 사이트에서 보안 연결 게이트웨이에 의해 아웃바운드로 시작됩니다. 이는 인터넷을 통한 업계 표준 TLS(Transport Layer Security) 256비트 암호화와 Dell Technologies Services에서 서명한 디지털 인증서 인증을 사용하여 안전한 종합 통신 터널을 생성합니다. 디지털 인증서는 안전한 현장 데이터 수집에 대한 이전 섹션에 자세히 설명되어 있습니다.

따라서 보안 연결 게이트웨이 연결에는 다음과 같은 속성이 있습니다.

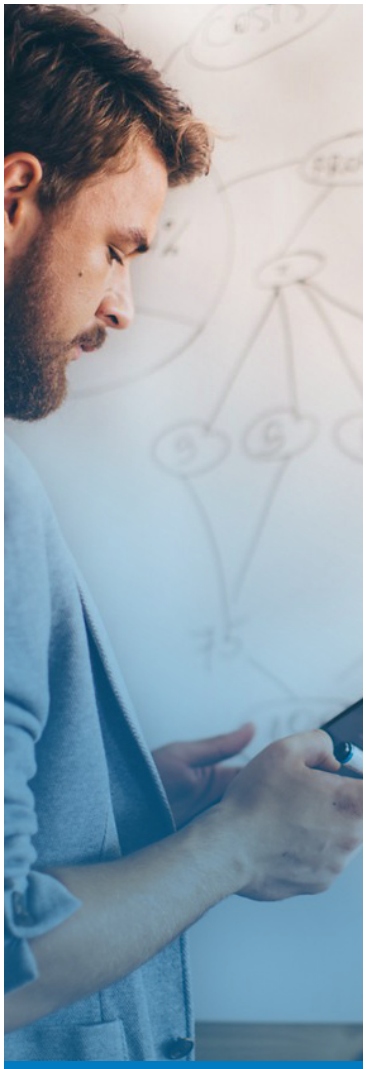
- **신뢰할 수 있는 데이터 전송:** 전송되는 각 메시지에는 메시지 인증 코드를 사용하는 메시지 무결성 검사가 포함되어 전송 중에 데이터의 탐지되지 않은 손실 또는 변경을 방지합니다.
- **TLS를 통한 비공개 세션 및 보안 세션:** 업계 표준 알고리듬을 사용하는 대칭 암호화는 각 연결에 대해 고유한 키를 생성합니다. 탐지되지 않는 협상 중에는 통신을 수정할 수 없습니다.
- **인증된 당사자**: 이 연결은 안전하기 때문에 공개 키 암호화를 사용하여 통신 당사자를 식별하고 인증합니다. 이 접근 방식을 사용하면 스푸핑과 MITM(Man-in-the-Middle) 공격을 방지할 수 있습니다.

안전한 TLS 터널을 사용한 통신

게이트웨이 서버는 TLS 터널을 사용하여 하트비트 폴링, 원격 알림 및 원격 액세스에 대한 안전한 환경을 보장합니다. 이 섹션과 다이어그램 C에는 Dell Technologies Services 기술의 자동화된 사전 예방적 및 예측적 환경을 위한 핵심적인 통신 프로세스와 프로토콜에 대한 자세한 내용이 나와 있습니다.

하트비트 폴링

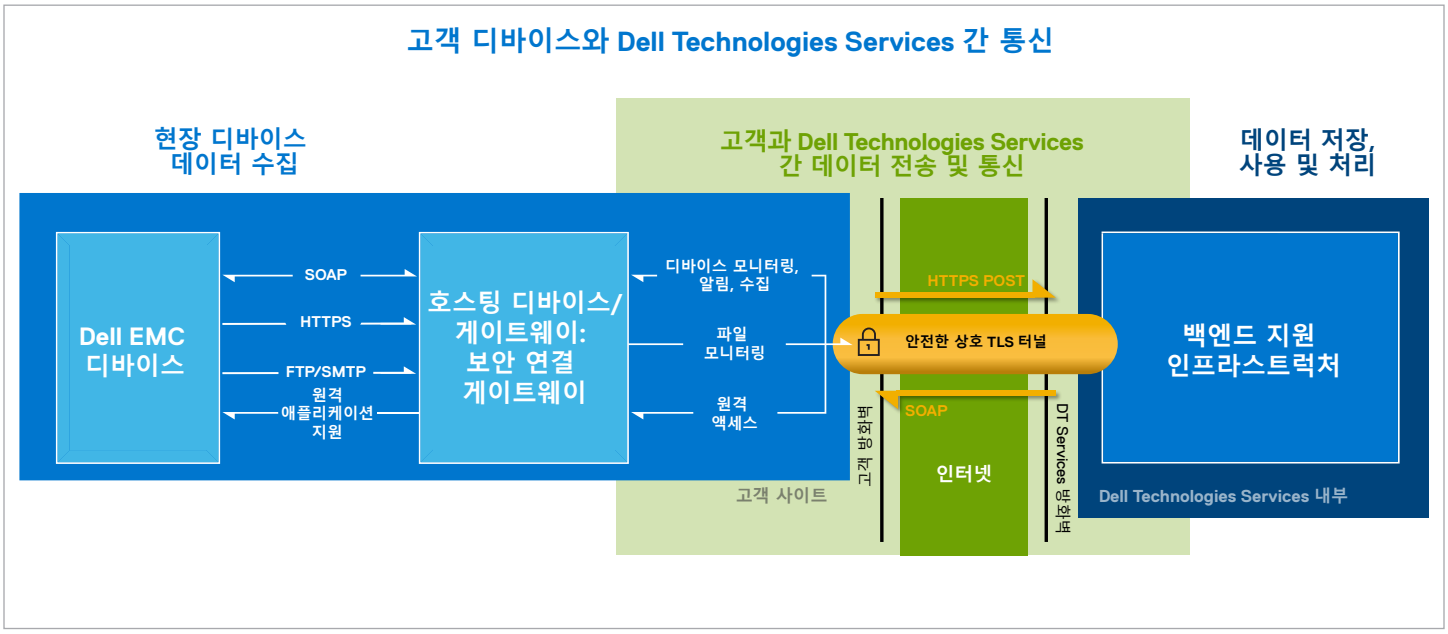
보안 연결 게이트웨이 환경의 이점을 누리려면 고객 시스템을 해당 환경에 연결해야 합니다. 하트비트 폴링은 디바이스의 연결 상태를 확인하고 수집된 텔레메트리 데이터를 백엔드에 정기적으로 전달합니다. 또한 데이터는 보안 연결 게이트웨이가 배포되는 게이트웨이 서버를 식별합니다.



업계를 선도하는 인증을 통해 스푸핑 및 MTM(Man-in-the-Middle) 공격으로부터 연결을 보호합니다.

안전한 TLS 터널을 사용한 통신(계속)

다이어그램 C: 보안 아키텍처



원격 알림 또는 Connect Home 기능

보안 연결 게이트웨이는 디바이스에서 이벤트 파일을 백엔드에 전송하는 안전한 통로 역할을 합니다. 여기에는 오류, 알림, 경고 조건, 상태 보고서, 구성 데이터 및 스크립트 실행 상태가 포함됩니다.

- 알림이 생성되면 이벤트 파일이 생성되고 게이트웨이로 전송됩니다.
- 이 파일은 HTTPS 수신기 서비스를 통해 보안 연결 게이트웨이에서 수신합니다.
- 보안 연결 게이트웨이에 FTP 및/또는 SMTP 수신기를 사용하는 기존 제품의 경우 파일이 암호화된 후 전송됩니다.
- 게이트웨이는 파일을 압축하여 TLS 터널을 통해 백엔드에 전송한 다음 수신기 디렉토리에서 파일을 삭제합니다.
- 그런 다음 분석을 위해 파일을 백엔드에서 압축 해제합니다.
- 보안 연결 게이트웨이는 암호화된 통신 터널을 통해 파일을 백엔드로 전송할 수도 있습니다. 또한 페일오버 채널, 즉 FTPS 또는 고객 이메일 서버를 사용하도록 게이트웨이를 구성할 수 있습니다.

시스템 모니터링 데이터는 실행 중인 시스템의 다양한 구성 요소에서 수집되어 Dell Technologies Services를 통해 지능적이고 빠른 적응형 지원 경험을 제공합니다. 작업 중인 특정 시스템을 식별하는 데 필요한 시스템 ID는 디바이스에서 수집된 회사와 관련된 유일한 정보입니다. 부품을 사전 예방적으로 구비해야 한다고 판단하는 경우에는 Dell Technologies 서버에 안전하게 저장된 기존 연락처 정보를 사용합니다.

일상적인 24시간 주기에서 벗어나 수집된 데이터를 포함하여 실행 중인 시스템에서 수집된 시스템 모니터링 데이터의 전체 목록은 보안 연결 게이트웨이의 보고 가능 항목 문서 및 OpenManage Enterprise용 서비스 플러그인에서 확인할 수 있습니다.

원격 액세스

또한 기술 지원 팀은 고객 사이트의 디바이스에 원격으로 액세스하여 문제를 해결하거나 디바이스 관련 작업을 수행합니다. 원격 액세스 세션은 비동기식 메시징을 통해 고객 사이트의 보안 연결 게이트웨이에 의해 시작됩니다. 그 다음에는 안전한 원격 액세스 세션이 다음과 같이 설정됩니다.

- Dell Technologies Services 백엔드에서 세션 인증이 완료되면 기술 지원 에이전트가 서비스 요청 번호(사용 가능한 경우), 기타 디바이스 또는 사용자 ID를 비롯한 디바이스 액세스 권한을 요청합니다.
- 원격 액세스 요청은 게이트웨이가 디바이스의 하트비트 메시지를 백엔드로 전송하여 검색할 때까지 백엔드에서 대기합니다.
- 이에 대한 응답으로 백엔드 서버는 요청 정보, 백엔드 서버 주소 및 고유한 세션 ID가 포함된 응답을 전송하여 게이트웨이에 연결합니다.
- 보안 연결 게이트웨이는 로컬 저장소를 사용하여 디바이스의 로컬 IP 주소를 확인한 다음, 정책 관리자에서 캐싱된 정책을 확인하여 연결 권한을 검토합니다.
- 허용되는 경우, 보안 연결 게이트웨이는 백엔드 서버에 대한 별도의 영구 TLS 연결을 설정합니다. TLS 연결은 항상 게이트웨이에 의해 시작됩니다. 백엔드 서버는 게이트웨이 서버에 대한 인바운드 연결을 시작할 수 없으므로 외부 공격에 대한 취약성이 없습니다.

통신은 종료되거나 비활성 상태로 일정 시간이 지나 시간 제한에 도달할 때까지 보안 연결 게이트웨이와 백엔드 서버 간의 터널을 통해 이루어집니다.

네트워크 보안

모든 네트워크 모니터링 구성 요소는 방화벽 뒤에 위치하며 네트워크 보안 팀에서 관리합니다. 네트워크 트래픽은 엄격하게 관리됩니다. 모든 인바운드 트래픽은 특정 포트를 통해 전송되며 적절한 대상 네트워크 주소로만 전송됩니다.

4-3: 안전한 데이터 저장, 사용 및 처리

저장 및 사용을 위한 보안

물리적 보안

Dell Technologies Services는 애플리케이션, 시스템, 네트워크 및 보안 구성 요소를 포함한 대부분의 보안 연결 게이트웨이 데이터를 높은 수준의 가용성과 보안을 유지할 수 있도록 설계된 미국 데이터 센터에서 호스팅합니다. 데이터는 물리적 보안을 비롯하여 다양한 수단을 사용하여 보호됩니다. 특징은 다음과 같습니다.

- 온프레미스 보안 경비원
- 카메라
- 가짜 출입문
- 차량 차단기
- 특수 주차장 설계
- 방탄 유리 및 방탄 벽
- 표시가 없는 건물 사용

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

논리적 보안

보안 연결 게이트웨이에 의해 생성된 데이터는 Dell 개인 정보 처리 방침에 따라 저장됩니다.

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

논리적 보안(계속)

- **서버 및 데이터베이스 보안:** 서버와 운영 체제 구성 요소는 보안 검토가 이루어진 표준 이미지에 상주합니다. Microsoft 및 기타 소프트웨어 공급업체에서 게시한 보안 업데이트를 포함하여 애플리케이션에서 사용하는 보안 업데이트에 대한 정기적인 검토가 있습니다. 중요한 보안 업데이트를 게시하는 경우 먼저 운영 이미지가 아닌 이미지를 테스트한 다음 적절한 시기에 라이브 서버에 정식 적용하여 위험을 방지합니다.
- **감사:** 모니터링 대상 디바이스 로그는 승인된 Dell Technologies Services 인프라스트럭처 및 애플리케이션을 통해서만 액세스할 수 있습니다. 이러한 로그는 운영 체제 또는 보안 연결 게이트웨이 웹 서버 콘솔에 로그인하거나 액세스하는 모든 시도를 기록합니다.

IT 부서에서 관리하는 빌드는 권장 CIS(Center for Internet Security) 제어 보안 모범 사례를 사용하여 강화됩니다. 업계 표준 보안 지침도 모든 서버 및 네트워크 장비에 구현되어 있습니다.

마지막으로, 보안 연결 게이트웨이 지원 환경은 데이터 센터 내 로컬 고가용성과 별도의 데이터 센터에 있는 동일 인프라스트럭처를 모두 사용합니다. 유일한 예외는 빅데이터 클러스터와 프라이빗 클라우드와 같은 본질적으로 가용성이 높은 기술입니다. 데이터 분석의 경우 Dell Technologies Services는 프라이빗, 하이브리드 및 퍼블릭 클라우드를 비롯하여 완벽하게 제어하고 관리할 수 있는 클라우드 환경을 활용합니다.

인증

보안 연결 게이트웨이는 Dell Technologies Services 인증에 Dell MyAccount를 사용하고 즉시 사용 가능한 인증에 OS 로그인 그룹을 사용합니다.

보안 연결 게이트웨이 구성 요소에 대한 액세스 권한이 있는 데이터베이스 관리 팀과 운영 지원 팀 등의 그룹에는 별도의 작업 및 액세스 권한이 할당됩니다. 운영 환경에 대한 모든 업데이트는 검사와 균형이 포함된 정해진 변경 관리 프로세스를 거칩니다.

제품 및 애플리케이션에 대해 반복 가능하고 안전한 개발 프로세스를 활용합니다.

처리를 위한 보안

보안 인식 제고 커뮤니티

작업별 보안 모범 사례와 관련 리소스 사용 방법에 대해 신규 직원과 기존 직원을 교육할 수 있는 여러 수준의 역할 기반 보안 교육 과정을 제공합니다. Dell Technologies는 전체 커뮤니티에서 보안을 의식하는 문화를 조성하고자 노력하고 있습니다. 또한 개발자 커뮤니티는 Dell의 보안 챔피언 프로그램의 일부이며, 이 프로그램은 소프트웨어 개발 관행을 통해 원점 회귀 보안을 촉진하도록 고안되었습니다.

개발

내부 **SDL(Secure Development Lifecycle) 표준**은 시장 기대치와 업계 관행에 따라 제품 및 애플리케이션의 안전한 개발 활동을 벤치마킹하는 Dell Technologies 제품 관련 조직을 위한 일반적인 참고 자료입니다. 이는 제품 팀이 새로운 기능을 개발할 때 도입해야 하는 보안 제어 조치를 정의합니다. SDL에는 두 분석 작업과 주요 위험 영역에 대한 규범적이고 사전 예방적인 제어 조치가 포함되어 있습니다. 위협 모델링, 정적 코드 분석, 검사 및 보안 테스트와 같은 분석 작업은 개발 수명주기 전반에 걸쳐 보안상의 결함을 탐색하고 해결하기 위한 것입니다. 규범적인 제어 조치는 개발 팀이 보호가 보장되는 방식으로 코딩하여 OWASP(Open Web Application Security Project) Top 10 또는 SANS Top 25에서 발견된 문제를 포함하여 일반적인 보안 문제를 방지하기 위한 것입니다. 보안 연결 게이트웨이는

개발(계속)

업계 표준에 맞춰 보안 제어 기능을 구현하기 위해 Dell SDL 성숙도 프레임워크를 채택했습니다.

보안 연결 게이트웨이 코드는 애자일 개발 방법론을 사용하여 개발됩니다. 코드는 업계 표준 자동화 소프트웨어를 사용하여 지속적으로 통합됩니다. 코드 버전은 보안 그룹 사용 권한을 사용하여 체크인 및 관리됩니다.

모든 소프트웨어 릴리스는 다음을 비롯하여 보안 정책에 따른 보안 평가를 거칩니다.

- 침투 테스트를 사용한 취약성 평가
- Secureworks와 같은 업계 최고의 여러 공급업체를 활용한 타사 보안 테스트
- 인증, 권한 부여 및 ID 관리 솔루션에 대한 평가
- 업계를 선도하는 소프트웨어 구성 요소 분석용 솔루션을 통해 모든 타사 라이브러리와 구성 요소 검사. 특정 보안 개선 사항을 위해 Dell 보안 권고 사항도 제공됩니다.
- 글로벌 보안 조직의 데이터 분류. 이 프로세스를 통해 개인 정보 보호 및 보안을 함께 제공하여 전자 데이터를 보호합니다.

애플리케이션은 보안 감사 및 거버넌스의 대상이기도 합니다.

변화 관리

Dell Technologies 변경 관리 프로세스는 기업 변경 관리 이사회에서 규정한 ITIL Foundation 모범 사례를 따릅니다. 모든 변경 사항은 변경 요청 티켓을 통해 관리됩니다. 변경을 시작하기 위해 시스템에 액세스하려면 ITIL 교육을 거쳐야 할 뿐만 아니라 SDL도 숙지해야 합니다. 백엔드 인프라스트럭처에 적용되는 모든 업데이트 및 업그레이드는 적절한 추적 및 추적 가능성을 위해 버전 관리가 적용됩니다. 팀에서는 자동화된 빌드 프로세스를 통해 새 빌드를 적용하거나 배포된 빌드 또는 핫픽스를 취소할 수 있습니다.

고객의 내부 환경에 설치된 애플리케이션은 고객의 선호도에 따라 업그레이드할 수 있습니다. Dell.com/support로 승격되는 모든 릴리스에는 알려진 제한 사항이 적용된 변경 사항에 대한 정보가 포함되어 있습니다.

새로운 모든 기능과 변경 사항은 제품 관리 팀에 의해 정리되며, 검토 및 승인을 위해 변경 관리 이사회를 거치는 POR(Plan-of-Record) 변경 프로세스를 통해 우선 순위가 지정됩니다.

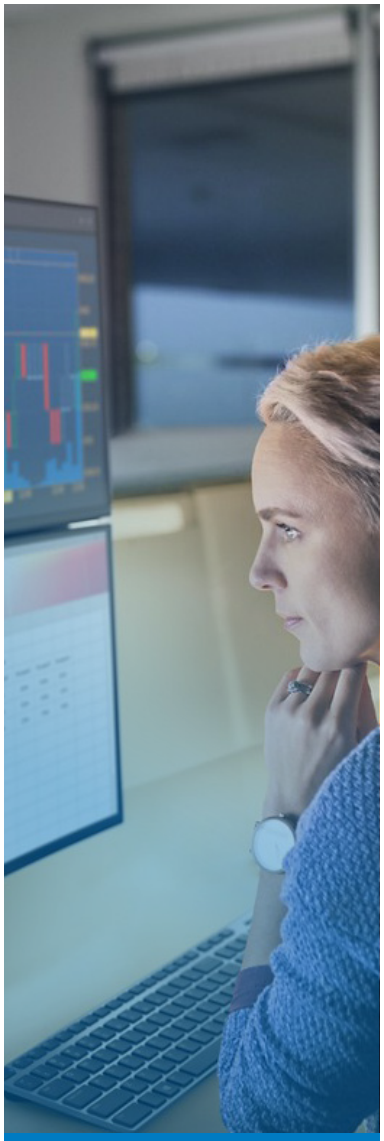
공급망 위험 관리

Dell Technologies는 계획-소싱-개발-제공-반환 수명주기의 각 단계에서 업계를 선도하는 모범 사례를 따릅니다. 글로벌 시장에서 신뢰할 수 있는 ICT 공급업체의 입지를 유지하기 위해 국제 SCRM 표준 및 모범 사례를 비롯하여 공급망의 보호하기 위해 종합적인 접근 방식을 사용하고 있습니다.

Dell 공급망 보증 관행에 대한 상세 정보는 여기를 참조하십시오.

인시던트 보고

의심스러운 활동을 목격하거나 사이버 보안 문제 또는 위협 요소를 의심하는 모든 Dell Technologies 사용자는 CSIRT(Computer Security Incident Response Team)에 즉시 인시던트를 보고해야 합니다. 여기에는 환경에 영향을 미치거나 시스템 및/또는 데이터 위반이 발생할 수 있는 보안 프로세스의 취약성 또는 격차가 포함됩니다. 그런 다음 CSIRT는 인시던트에 대한 전체 조회를 실행하고, 인시던트를 보고하는 인력은 CSIRT가 조사를 수행하는 데 필요한 모든 아티팩트와 세부 정보를 제공합니다. CSIRT 팀은 Dell 내부 사이버 보안 인시던트와 고객이 직면하지 않은 사이버 보안 인시던트에 대응하고 이를 해결하기 위한 공식 프로세스가 자세히 설명된 CSIRT 인시던트 대응 계획을 사용합니다. 이러한 인시던트는 Dell 자산, 컴퓨터 네트워크 또는 데이터 처리 장비는 물론 Dell과 해당 자회사, 직원, 서비스 공급업체, 파트너 또는 고객 정보에 대한 잠재적 위협을 제기할 수도 있습니다.



제품 보안 모범 사례에 대한 업계 협업

취약성 대응

Dell Technologies는 고객에게 취약성으로 인한 위협을 해결할 수 있는 정보, 지침 및 완화 조치를 적시에 제공하여 고객이 제품의 보안 취약성과 관련된 위험을 최소화하도록 최선을 다합니다. PSIRT(Product Security Incident Response Team)는 보고된 모든 제품의 취약성에 대한 대응 및 공개 사항을 조율하는 역할을 담당합니다. 모든 Dell Technologies 제품 취약성 공개 사항은 온라인으로 제공됩니다.

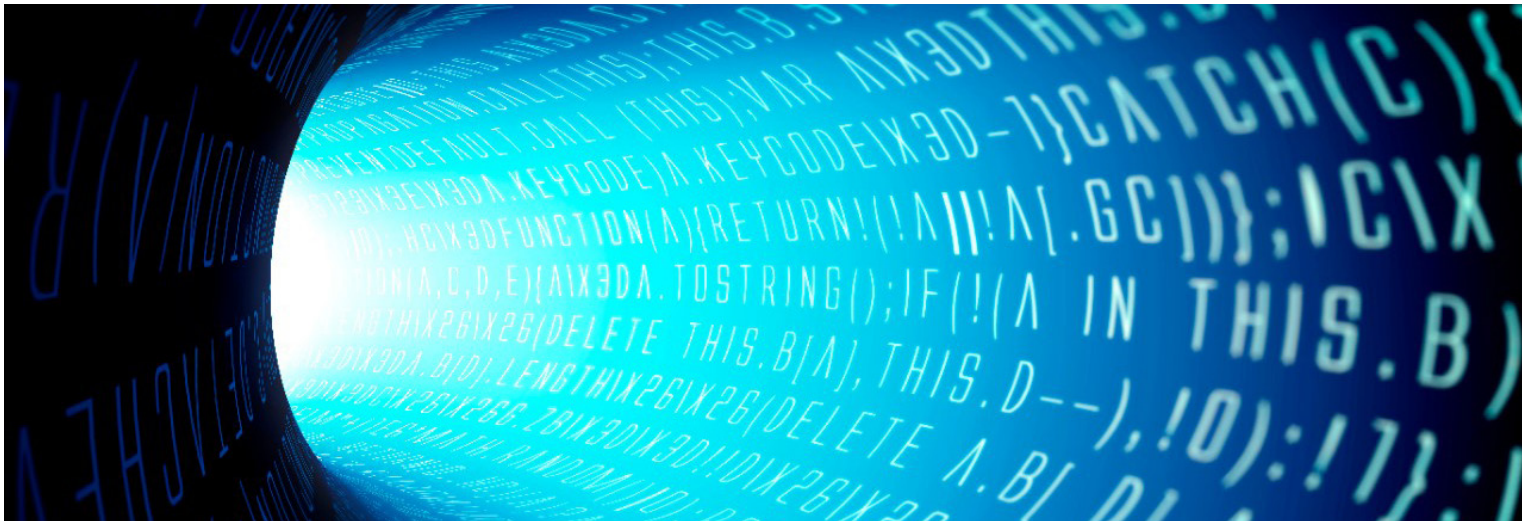
취약성 대응 정책에 대한 자세한 정보

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.

- Dell은 EMC 법인을 통해 SAFECode(Software Assurance Forum for Excellence in Code)를 공동 설립하고 현재 해당 이사회를 이끌고 있습니다. 다른 이사회 구성원으로는 Microsoft, Adobe, SAP, 인텔, Siemens, CA 및 Symantec이 있습니다. SAFECode 구성원은 소프트웨어 보증 관행 및 교육을 공유하고 게시합니다.
- Dell Technologies는 FIRST(Forum for Incident Response and Security Teams)에서 현재 활동하고 있는 구성원입니다. FIRST는 인시던트 및 취약성 대응 분야에서 최고로 꼽히는 조직이자 인정받는 글로벌 리더입니다.
- Dell Technologies는 OTTF(Open Group Trusted Technology Forum)에 적극적으로 참여하고 있습니다. OTTF는 글로벌 공급망 무결성 프로그램과 프레임워크 개발을 주도하고 있습니다.
- Dell은 2008년 BSIMM(Building Security In Maturity Model) 프로젝트에 의해 평가된 최초의 9개 회사 중 하나였으며 이 프로젝트에 계속 참여하고 있습니다. Dell Technologies 대표는 BSIMM 자문 위원회에 속해 있습니다.
- 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.

엔터프라이즈 보안 질문에 대한 답변을 찾는 데 도움이 되는 리소스 및 솔루션은 Security and Trust Center를 방문하시기 바랍니다.



업계 보안 표준

Dell 직원은 보안 표준을 개발하고 업계 차원의 보안 관행을 정의하는 데 중점을 두는 다음과 같은 업계 컨소시움에 적극적으로 관여합니다.

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

ISO 9001 인증

Dell Technologies는 ISO 9001 인증을 받았습니다. 당사는 모든 개발 및 제조 센터에 대해 정기적으로 분기별 감사와 규정 준수 검토를 수행합니다.

5: 결론

Dell Technologies의 연결 기술은 중요한 데이터 센터 인프라스트럭처의 최대 가동 시간을 보장하는 자동화된 사전 예방적 및 예측적 알림을 통해 간편한 IT 지원 환경을 제공합니다. Dell Technologies Services와 파트너 관계를 맺고 있는 고객은 텔레메트리 데이터의 수집, 통신, 전송, 사용 및 저장을 위한 안정적이면서 위험에 노출되지 않고 안전한 경험을 제공하겠다는 당사의 약속을 확신할 수 있습니다.

질문과 자세한 정보는 DellTechnologies.com/SecureConnectGateway를 방문하시기 바랍니다.

1 출처: Dell Technologies의 의뢰로 Forrester Consulting이 수행한 연구 결과, "The Role Of IT Services Providers Expands To Strategic Collaboration", 2021년 4월

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