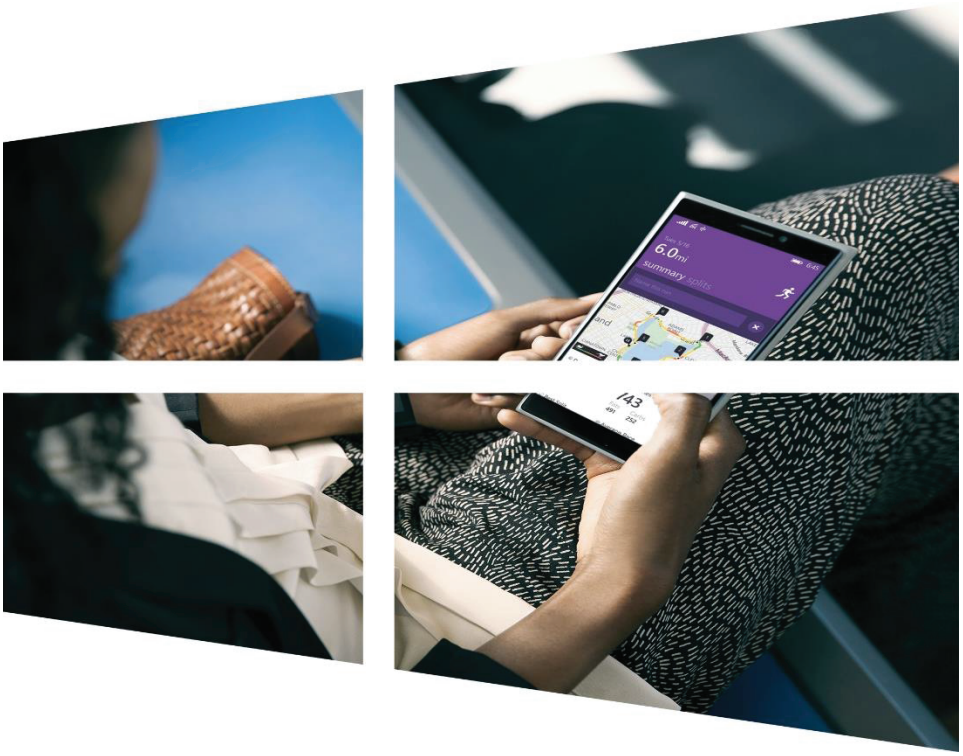
Windows 10



Windows 10 IoT 보안

초판 발행일: 2016년 7월 15일
개정 버전 2.0

개요

이 백서에서는 Windows 10 IoT Enterprise, Windows 10 IoT Mobile 및 Windows 10 IoT Core를 포함한 Windows 10 IoT 제품군이 다양한 장치 유형의 보안 요건을 충족시키도록 설계된 단일 플랫폼을 제공하는 방법에 대해 알아봅니다. 사물 인터넷(IoT)이 계속 진화하면서 보안 요구, 사용자 경험, 다양한 장치의 리소스 제약 등을 균형 있게 고려한 IoT 플랫폼을 토대로 장치를 구축하는 것이 점차 중요해지고 있습니다. Windows 10 IoT가 바로 이런 플랫폼입니다. Windows 10 IoT는 강력한 자격 증명(장치 ID와 사용자 ID 모두), 보안 데이터 및 보안 연결을 통해 견고한 보안 기능을 제공합니다. 이 백서에서는 IoT 보안의 주요 측면을 비롯해 OEM(Original Equipment Manufacturer)이 Windows 10 IoT를 통해 안전한 장치를 만들어서 고객 만족을 실현하고 있는 방법을 알아보겠습니다.

IoT 시대의 보안

오늘날 우리는 급속한 디지털 전환과 사물 인터넷(IoT)의 출현을 목도하고 있습니다. 이러한 디지털 전환 덕분에 스마트 IoT 장치들이 무한대로 연결되어 서로 활발하게 통신하는 환경을 구축할 수 있게 되었습니다. 장치 간의 연결로 인한 새로운 가능성의 출현이 이미 목도되고 있습니다. 향후 몇 년 동안 초소형 센서부터 초대형 산업용 플랫폼에 이르는 모든 장치의 혁신적인 통합이 계속 될 것입니다. 한편으로는 인터넷 초기에 네트워크 취약점이 대두되었던 것과 마찬가지로(퇴치를 위한 보안책이 마련되기도 전에 취약점이 속속 등장), 사물 인터넷을 둘러싼 보안 우려에 대한 인식이 높아질 것입니다. 현재로서는 IoT 장치의 급속한 확산과 통합에 대한 낙관주의로 인해 광범위한 장치에서 나타날 수 있는 실질적인 보안 위험을 간과하기 쉬워질 수 있습니다. 그러나 IoT가 계속 성숙해감에 따라 보안에 대한 관심도 높아질 것입니다.

IoT 장치는 중요한 데이터를 생성, 소비 및 집계하는 네트워크 에지에 위치합니다. 이들 장치에서 ID와 데이터가 유출되는 일이 없도록 하려면 견고한 보안 기능이 필요합니다. 현재는 장치 보안을 위한 특정한 IoT 보안 표준이 존재하지 않습니다. 장치가 처음부터 보안을 고려해 설계되도록 만드는 프레임워크가 구축되어 있지 않으면 기업의 기술 에코시스템에 새 장치가 추가될 때마다 새로운 취약점이 등장하게 됩니다. 사물 인터넷을 보호하고 최대한 활용하는 것이 중요하며, Windows 10 IoT는 IoT의 이점을 안전하게 실현할 수 있도록 지원하는 첨단 플랫폼 역할을 하도록 설계되었습니다.

사물 인터넷을 보호하고 최대한 활용하는 것이 중요하며, Windows 10 IoT는 IoT의 이점을 안전하게 실현할 수 있도록 지원하는 첨단 플랫폼 역할을 하도록 설계되었습니다.

미래의 장치는 쉽게 익혀서 대량 채택이 가능하도록 설계 및 마케팅되기 때문에 앞으로는 장치 통합이 비즈니스 및 개인 생활의 민감한 부분까지 적극적이고 심도 깊게 이루어질 것입니다. 그 결과, 보안에 대한 사고의 전환이 이미 진행 중에 있습니다. 공공 영역에서 데이터 보안 및 개인 프라이버시에 대한 우려가 높아지면서 견고하게 설계된 보안이 점차 비즈니스의 필수 과제로 떠오르면서 마케팅되고 있습니다. 이러한 프로세스는 엔터프라이즈 시스템에 이미 뿌리를 내리고 있습니다. 예를 들어 엄격한 통제에 대한 요구로 인해 대규모 시스템이 보안을 고려해 설계되고 있습니다. IoT 프레임워크 내에서 다양한 장치 유형이 수행하는 역할에 대한 인식이 높아지면서 가장 견고한 보안 기능을 제공하는 IoT 장치를 둘러싸고 비슷한 시장이 형성될 것으로 보입니다. 전통적으로 보안 대책의 구현은 사용자 경험에 장애물이 되었습니다. 보안은 설계와 병행해야 하는 것으로 인식되기 보다는, 오히려

불편한 요구 사항으로 간주되었습니다. 기본적인 보안을 위해서는 장치 기능에 대한 사용자 경험에 부정적인 영향을 미치지 않으면서 위험과 위협을 처리하는 견고한 보안 설계가 수반되어야 합니다. 업계 선도적인 IoT 플랫폼이라면 사용자 경험의 품질을 저하시키지 않으면서도 보안을 제공하여 한 걸음 더 나아갈 수 있게 해야 합니다.

IoT 장치의 보안에 대한 관심이 높아지면서 보안을 고려한 설계와 혁신이 이루어지는 만큼, 비즈니스 환경 내의 모든 장치에 동일한 보안 플랫폼을 제공하고 상호 운영성을 보장하는 것의 중요성도 높아질 것입니다. IoT에 대해서는 여전히 미숙한 상태이기 때문에 IoT 장치를 위한 범용 보안 표준은 아직 등장하지 않았습니다. 이기종 보안 플랫폼을 위해 설계된 장치들은 취약점을 야기하기 쉬울 것이며, 상호 운영성이 부족한 장치들은 표준화로 인해 어려움을 겪을 것입니다. 상호 연결된 기술 에코시스템을 위해 견고하게 통합된 보안 제어 및 지원을 제공하는 플랫폼을 활용하는 장치 제조업체들은 경쟁 우위를 누리게 될 것입니다.

다양한 장치 유형에 해당되는 비즈니스 시나리오 및 리소스 제약을 수용하는 IoT 플랫폼이 필요합니다. 스마트 장치를 안전하게 통합하고자 하는 양심적인 장치 제조업체와 기업들은 많은 IoT 구성 요소에 대해 리소스 제약을 둘 것입니다. 환경 센서와 같은 소형의 로우엔드 장치들은 경량형이기 때문에 기존 시스템(PC, 핸드폰 등)에서 이용할 수 있는 전원, 메모리, 스토리지 및 암호화 기능을 갖추고 있지 못합니다. 판매 이후 소형 장치에 보안 기능을 추가하는 것은 위험하고 복잡하기 때문에 최종 사용자는 제조업체가 이러한 리소스 제약에도 불구하고 즉시 적용 가능한 보안 기능(강력한 장치 ID, 조작 방지, 원격 검증, 암호화 등)을 완벽하게 보완할 수 있는 방법을 찾아주기를 기대할 수밖에 없습니다.

엔터프라이즈급 플랫폼은 다양한 장치 리소스 제약, 보안 요구, 사용자 경험을 균형 있게 고려해야 합니다. 기능적으로 볼 때 엔터프라이즈급 보안 플랫폼은 보안 ID, 보안 데이터 및 보안 연결을 제공하고 확인할 수 있어야 합니다. Windows 10 보안 플랫폼은 이러한 3가지 요소를 모두 충족하도록 설계되었습니다.

Windows 10은 견고한 보안 장치 ID, 보안 사용자 ID 및 보안 연결을
제공하도록 설계되었습니다.

보안 ID

적절한 IoT 보안을 위해서는 장치 자체에 강력한 보안 사용자 ID와 강력한 보안책이 내장되어 있어야 합니다. Windows 10은 사용자 ID와 장치 ID를 모두 보호할 수 있도록 혁신적인 기능을 제공하고 있습니다.

보안 장치 ID

대부분의 IoT 환경에서는 연결 장치들이 서로 끊임 없이 통신합니다. 일반적으로 사용자 상호 작용 없이도 지속적으로 통신이 이루어집니다. 통신을 위한 지속적인 액세스 권한을 부여 받은 장치는 자격 부여를 위한 초기 핸드셰이킹 이후에도 보안이 유지되어야 합니다. 보안 프로토콜과 암호화된 통신을 사용한다고 해서 신뢰가 보장되는 것은 아닙니다. 왜냐하면 역사적으로 이러한 메커니즘들은 공격자가 장치에 실제 액세스하지 않는다는 가정 하에서 작동해왔기 때문입니다. IoT 장치 외부에만 보안을 구현하는 것으로는 충분하지 않다는 것이 Microsoft의 견해입니다. 이들 장치에 견고한 보안 기능을 내장해야 합니다.

Windows 10 은 각 장치에 보안성과 복원성이 기본적으로 지원되어 고객 데이터와 프라이버시를 보호하고 보안 침해 시에도 다른 시스템에 대한 액세스를 제한할 수 있는 경우에만 시스템에서 엔터프라이즈급 보안이 실현된 것으로 봅니다. 더 나아가 사용자는 Windows 10 내의 고급 보안 제어 기능을 통해 장치 유형을 기준으로 장치 ID 프로토콜을 구분할 수 있습니다. 따라서 리소스 제약 및 비즈니스 시나리오를 수용하면서도 보다 민감하고 미션 크리티컬한 장치에 보다 확실한 수요를 적용할 수 있도록 적절한 보안 프로토콜을 통해 하위 수준 장치(예: 온도 센서)를 식별할 수 있습니다. 이러한 포괄적인 보안 기능들은 리소스 제약에 관계 없이 모든 장치 ID를 보호 및 확인할 수 있도록 지원합니다.

IoT 디바이스 외부에만 보안을 구현하는 것으로는 충분하지 않다는 것이 Microsoft의 견해입니다. 이들 장치에 견고한 보안 기능을 내장해야 합니다.

보안 사용자 ID

Windows 10 IoT는 장치의 보안성을 모니터링 및 확인할 수 있다는 점에서 안전한 사용자 ID를 보장할 수 있는 새로운 기회를 열었습니다. 과거에는 보안 데이터에 액세스할 수 있으려면 먼저 사용자에게 ID 정보(암호, 핀 등)를 제공하도록 요구하는 데 인증 노력이 집중되었습니다. 그러나 이러한 인증 모델은 통신 채널에 보안 침해가 발생하지 않도록 하기 위해 ID 정보를 안전하게 유지하고 강력한 암호를 사용할 책임을 사용자의 몫으로 돌립니다. 하지만 이 방법의 경우, 아무리 여러 정보를 요구하더라도 가장 취약한 지점에 따라 보안 수준이 결정됩니다. Windows 10 IoT의 장치 ID 보안 방법에서는 장치 자체를 MFA(Multi-Factor Authentication) 모델의 한 요소로 사용할 수 있습니다. 즉, 보다 확실한 인증을 위해 장치에 자격을 부여할 때 물리적 근접성, 상호 작용 여부, 상호 연관된 보안 장치 등의 인증 요소를 추가할 수 있습니다. 핀 또는 생체 인식 지원(안면, 홍채 및 지문)이 함께 이루어지면 보안 장치(휴대폰 또는 스마트 와치)는 가장 강력한 인증 방법을 제공할 수 있고, 궁극적으로 단일 요소를 지배적인 사용자 인증 방법으로 사용하던 것에서 탈피할 수 있습니다.

보안 데이터

데이터는 보관 중일 때나 이동 중일 때나 보안이 유지되어야 합니다. Windows 10 IoT 보안 철학은 계층화된 접근 방식을 토대로 합니다. 즉, 사용자는 기록된 볼륨 자체가 분실 또는 도난으로 인해 침해되더라도 데이터가 취약하지 않다는 것을 신뢰할 수 있어야 합니다. Windows 10 IoT는 Windows 10 IoT 장치에서 전체 시스템 볼륨과 분할된 모든 데이터 볼륨을 암호화하는 Microsoft의 업계 선도적인 전체 디스크 암호화 기술을 통해 사용자의 데이터를 보호합니다.

보관 중인 데이터에 대한 포괄적인 암호화는 기록된 볼륨이 침투 당하지 않도록 보호합니다. 그러나 총체적인 데이터 보안책은 여기에서 끝나지 않습니다. Windows 10 IoT의 보안 플랫폼은 아래 나와 있듯이 보관 시는 물론 이동 시에도 데이터 보안을 보장하도록 설계되었습니다.

보안 연결

민감한 정보를 교환할 때 IoT 장치 간의 통신이 보호되도록 보장하는 것이 Windows 10 IoT 보안 플랫폼의 세 번째 핵심 요소입니다.

Windows 10 IoT는 기본적으로 산업용 장치와 모바일 장치 간의 통신에 있어 여러 암호화 방법을 지원하도록 설계되었고, 리소스 제약이 있는 장치에서도 통신 프로토콜을 지원하여 연결된 장치 유형에 관계 없이 취약점을 차단할 수 있도록 지원합니다.

Windows 10 IoT 기능이 어떻게 장치 ID를 보호하는지 자세히 이해하기 위해 Contoso의 몇 가지 장치 시나리오를 살펴보겠습니다.

Contoso 시나리오 사례

Windows 10 IoT의 이점을 활용한 덕분에 Contoso는 ATM 트랜잭션을 보다 편리하고 안전한 방식으로 수행함으로써 고객을 확보할 수 있게 되었습니다. Contoso는 고객의 ATM 경험에 통합하는 방법으로 모바일 뱅킹 앱을 개선했습니다. 모바일 뱅킹 앱을 통해 사용자는 ATM에 직접 가지 않고도 자신의 휴대폰에서 ATM 트랜잭션의 대다수를 처리할 수 있게 되었습니다. 고객들은 모바일 장치에 대한 완벽한 제어권을 갖기 때문에 언제든 개인적으로 편리하게 Contoso 모바일 뱅킹 앱과 상호 작용할 수 있습니다.

Contoso의 고객 ID 보호

Contoso는 오늘날의 보안 환경에서는 취약한 사용자 이름 및 암호를 통해 고객 ID를 확인하는 것만으로는 충분하지 않다는 것을 잘 알고 있습니다. 이에, Contoso는 고객 계정 및 ID에 대한 무단 액세스를 차단할 수 있는 다계층 접근 방식을 구현했습니다. 이러한 접근 방식의 하나로 MFA(Multi-Factor Authentication)를 채택하고 있습니다. 고객들은 ID 확인을 위한 보조 양식(예: 이메일 또는 텍스트를 통해 고객에게 전송되는 1회용 암호)을 작성한 이후에만 모바일 뱅킹 앱에서 첫 번째 등록을 완료할 수 있습니다. 장치가 Windows Hello와 호환되는 하드웨어를 가지고 있는 경우에는 생체 인식 인증(안면, 홍채, 지문)을 사용하여 기존 암호로는 불가능했던 방식으로 ID를 확인할 수 있습니다.

고객이 트랜잭션을 제출하면 앱은 2차원 바코드를 생성하고, 고객은 이를 ATM에서 스캔합니다. 더 이상 PIN을 입력하고 메뉴를 탐색하는 동안 불안해 할 필요가 없고, 핀 및 은행 카드 정보 탈취를 위해 ATM에서 ID 도용이 발생하지 않았을까 걱정할 필요가 없습니다. 현금이 나오면 전체 거래가 신속하게 완료됩니다. Contoso의 고객들은 더 안전하고 쉬워진 새 ATM의 보안에 대해 만족하고 있습니다. Contoso가 자신의 ID와 금융 정보를 취약점으로부터 보호하도록 설계된 고급 기술을 구현했다는 점을 고객들이 인식하게 되면서 고객 충성도가 높아집니다.

ATM 키오스크 애플리케이션과 Contoso의 클라우드 소프트웨어 간의 통신 보호

보안 및 견고한 기능에 대한 Windows 10 IoT의 계층화된 접근 방식 덕분에 강력한 보안을 고려하여 사물 인터넷을 설계할 수 있었다는 사실에 대해 Contoso 역시 만족스럽게 생각합니다. ATM 장치의 애플리케이션은 첨단 암호화 및 전송 보안 프로토콜을 통해 Contoso의 백엔드 클라우드 애플리케이션과 통신을 함으로써 장치에 로컬로 상주하는 애플리케이션과 데이터의 수를 줄일 수 있게 지원합니다. 클라우드에 소프트웨어를 호스팅하는 것은 Contoso에게는 경제적인 방법입니다. 왜냐하면 수천 대에 달하는 장치에서 소프트웨어를 관리 및 유지보수하는 데 드는 비용을 상당수 줄일 수 있기 때문입니다. ATM 애플리케이션과 Contoso의 클라우드 애플리케이션 간의 통신은 VPN 기능인 보안 원격 액세스(Secure Remote Access)에 의해 보호됩니다. 이 기능은 클라우드와 ATM에 설치된 애플리케이션 간에 보안 연결을 설정하기 위해 애플리케이션별로 작동합니다. 더 나아가 Contoso는

네트워크에 연결 중이거나 네트워크를 통과하는 모든 장치의 시스템 상태를 평가하고 규정 미준수 장치를 검역하는 네트워크 액세스 보호(Network Access Protection)와의 통신을 보호합니다. Contoso는 Windows Firewall을 사용하여 원치 않는 네트워크 통신을 적극적으로 차단하고 있습니다.

Windows 10 IoT에서 Contoso는 공용 네트워크에서 데이터를 안전하게 암호화 및 전송할 수 있도록 지원하는 최신 TLS(Transport Layer Security) 암호화 프로토콜을 통해 항상 업데이트 상태를 유지하고 있습니다. 엔터프라이즈 장치에서 Windows 10은 최신 VPN 기술을 제공합니다.

Contoso의 ATM 키오스크 애플리케이션 보호

Windows 10 IoT 덕분에 Contoso는 ATM 키오스크 애플리케이션의 보안성을 개선하는 동시에, 일관되고 예측 가능한 사용자 경험을 구축할 수 있었습니다. 어쨌든 ATM은 그 성격 상 무인 장치입니다. 따라서 우발적인 리셋이나 고의적인 리셋에 취약합니다. IoT 장치에 대한 포괄적 보안이란 상상할 수 있는 모든 시나리오를 계획하여 다운타임을 최소화하는 것을 의미합니다. Windows 10 IoT는 처음부터 예기치 않은 재부팅으로 인해 장치 및 데이터 보안이 침해되는 일이 없도록 설계되었습니다.

적절한 사용자 경험을 제공하려면 Contoso가 ATM 키오스크 애플리케이션에서 원하는 애플리케이션이 바로 시작되도록 보장해야 합니다. 이를 위해 Contos는 Shell Launcher를 사용하여 시작 화면을 억제하고 Contoso의 전용 ATM 키오스크 애플리케이션이 바로 시작되도록 함으로써 침입을 방지하고 있습니다. UWP(Universal Windows Platform) 앱을 실행하기 위해 동일한 기능이 존재하는데, 시작 화면을 억제하고 앱을 바로 시작하기 위해 App Launcher를 사용하고 단축 키, 터치 제스처 및 기타 방법을 통해 사용자가 앱을 닫거나 끄는 것을 제한하는 정책을 실행하기 위해 Assigned Access를 사용합니다.

Contoso의 ATM의 전원이 꺼져서 재시작되는 경우, UWF(통합 쓰기 필터)는 예측 가능하고 안정적인 사용자 경험을 위해 Contoso의 ATM 키오스크 애플리케이션을 재시작 시와 똑같은 상태로 복귀시킵니다. UWF는 보호 볼륨에 대한 모든 쓰기를 인터셉트하여 오버레이에 기록함으로써 재시작 시에 계속 적용되지 않도록 합니다. UWF는 예외 기능을 제공하여 원하는 변경 사항이 계속 적용되도록 합니다. 따라서 IT 관리자는 파일, 폴더 또는 레지스트리 키를 지정하여 쓰기 필터를 통해 계속 적용되도록 할 수 있습니다. Microsoft System Center 2012 플랫폼의 구성 요소인 System Center Configuration Manager는 "쓰기 필터 인식"이 가능하기 때문에 업데이트가 다운로드 되기 전에 장치에서 쓰기 필터를 껐다가 업데이트를 적용한 다음에 쓰기 필터를 다시 켤 수 있습니다. Windows 10은 이러한 읽기 전용 장치의 보안 기능 및 관리를 간소화하여 Contoso가 원하는 사용자 경험을 실현할 수 있도록 지원합니다.

Contoso는 신뢰할 수 없는 애플리케이션이나 파일로부터 ATM을 보호해야 합니다. AppLocker에서 Windows 10 IoT가 지원되기 때문에 Contoso는 실행이 가능한 앱 및 파일(실행 파일, 스크립트, Windows Installer 파일, DLL[Dynamic-Link Library], 패키지형 앱, 패키지형 앱 설치 프로그램)을 세분화해서 관리할 수 있게 되었습니다. 뿐만 아니라, Device Guard는 ATM에 보안 침해가 발생한 경우에 신뢰할 수 없는 소프트웨어(제로데이 악성 코드를 포함)가 실행되지 않는 구성 상태를 만들어서 또 다른 보호 계층을 추가합니다. Contoso는 Device Guard가 ATM 키오스크에서 신뢰할 수 있다고 생각하는 소스에 대한 제어권을 갖고 있으며, Device Guard에는 소프트웨어 공급업체가 원래 서명하지 않았을 수 있는 UWP 또는 Win32 앱에도 손쉽게 서명할 수 있도록 지원하는 도구가 함께 제공됩니다. 중요한 것은 AppLocker가 Windows 보안 관리 컨트롤 내에 존재하더라도 Device Guard가 운영 체제 밖에서 지원되기 때문에 맬웨어 침투에 대한 중첩 방어를 구축할 수 있다는 사실입니다.

실제 ATM 기기 보호

또한 Contoso는 물리적 침입으로부터 ATM을 보호해야 합니다. 여기에는 미승인 주변 장치로 인한 취약점과 데이터 손실의 위험을 줄임으로써 무인 ATM을 보호하는 것이 포함됩니다. Windows 10 IoT는 USB 정책에서 지원이 되기 때문에 미승인 USB 주변 장치로부터 장치를 보호할 수 있습니다. Contoso의 IT 인력은 원하는 USB 장치를 승인할 수 있기 때문에 승인된 비즈니스 사용에 차질을 빚지 않으면서 미승인 주변 장치 사용으로부터 키오스크를 보호할 수 있습니다.

ATM이 실제 손상을 입은 경우, Contoso는 Microsoft의 전체 디스크 암호화 기술인 BitLocker를 통해 장치를 보호합니다. 이 기술은 권한이 없는 사용자가 분실, 도난 또는 부적절하게 폐기된 컴퓨터에서 Windows 파일 및 시스템 보안을 침해하지 못하게 함으로써 데이터를 보호합니다. Contoso는 MDM(Mobile Device Management)을 사용하여 장치를 변경 또는 업데이트할 수 있는 사용자의 능력을 판단하는 사용자(서비스 기술자 또는 지점 내 ATM을 담당하는 지점 관리자)에 대한 정책을 설정하여 ATM 장치에 대한 데이터를 추가적으로 보호할 수 있습니다. 또한 Contoso는 MDM을 통해 로그를 조회하여 기술자에 의한 적절한 변경이든 침입자에 의한 변경이든 장치 변경이 이루어졌는지 여부를 확인할 수 있습니다. 장치 도난 시 Contoso의 MDM 정책은 Contoso의 사전 결정된 트리거 기준에 따라 시스템 셧다운과 더 나아가 데이터 완전 삭제를 개시하게 됩니다.

Contoso의 IoT 에코시스템은 여기에서 그치지 않고 다양한 소형 환경 센서를 추가하여 각 ATM의 상황을 모니터링하는 등 Windows 10 IoT의 유연성과 이점을 활용할 수 있는 기회를 모색했습니다. 이들 장치는 온도 및 조명 같은 요인에 대한 데이터를 수집하여 구체적인 시스템 상태를 은행에 다시 보고합니다. 스캐너와 근접 센서는 통행자 수와 다양한 광고 옵션에 대한 이들의 반응을 분석합니다. 이러한 모든 소형 장치들은 은행의 클라우드 시장 분석 애플리케이션에 대한 중계를 책임지고 있는 게이트웨이 장치와 데이터를 공유합니다.

이러한 센서 에코시스템을 점화하기 위해 Windows 10 내의 고급 보안 제어 기능을 통해 장치 유형을 기준으로 장치 ID 프로토콜을 구분할 수 있습니다. 따라서 리소스 제약 및 비즈니스 시나리오를 수용하면서도 보다 민감하고 미션 크리티컬한 장치에 보다 확실한 수요를 적용할 수 있도록 적절한 보안 프로토콜을 통해 하위 수준 장치(예: 온도 센서)를 식별할 수 있습니다. Windows 10 IoT를 실행 중인 초소형 장치들조차도 업계 표준 TPM(Trusted Platform Module)을 지원할 수 있습니다.1 별개의 애플리케이션이나 TPM 기반 펌웨어 애플리케이션은 인증, 보안 키 저장 및 정책 기반 키 사용을 위한 강력한 하드웨어 바운드 암호화 ID의 토대를 제공하는 것은 물론이고, 조작 방지 플랫폼 측정을 사용한 플랫폼 무결성 및 상태 증명을 제공합니다. 이러한 보안 기능들은 리소스 제약에 관계 없이 모든 장치 ID를 보호 및 확인할 수 있도록 지원합니다.

각 장치에 보안성과 복원성이 기본적으로 지원되어 고객 데이터와 프라이버시를 보호하고 다른 시스템에 대한 액세스를 제한할 수 있다는 점에서 Contoso의 시스템은 안전합니다. 고객들도 여기에 만족하고 있습니다. 보안 및 견고한 기능에 대한 Windows 10 IoT의 계층화된 접근 방식 덕분에 강력한 보안을 고려하여 사물 인터넷을 설계할 수 있었다는 사실에 대해 Contoso 역시 만족스럽게 생각합니다.

결론

사물 인터넷이 계속 진화하면서 보안 요구, 사용자 경험, 다양한 장치의 리소스 제약 등을 균형 있게 고려한 IoT 플랫폼을 토대로 장치를 구축하는 것이 점차 중요해지고 있습니다. 이를 염두하여 Windows 10 IoT는 저가의 소형 장치부터 정교한 산업용 기계에

이르는 다양한 장치 유형의 보안 요구 사항을 고려해 설계된 단일 플랫폼을 제공합니다. Windows 10 IoT는 사용자와 장치 ID, 데이터 및 연결을 보호할 수 있도록 엔터프라이즈급 보안 기능을 제공합니다. Windows 10 IoT를 사용하면 고급 보안 기술을 이용하여 오늘날 요구되는 사물 인터넷을 구축하고, 끊임 없이 혁신하는 플랫폼을 활용하여 미래의 요구를 충족할 수 있습니다.

[1] Windows 10에는 TPM 2.0 이상이 필요합니다.