BeyondTrust

ISMS-P와 연계 한 ID(신원) 보안 통제 정렬

본 문서는 정보 제공을 목적으로 하며, 한국 조직이 ISMS-P 요구 사항에 따른 자체 의무를 이행하는 데 BeyondTrust 제품을 어떻게 활용할 수 있는지에 대한 가이드를 제공합니다. BeyondTrust는 거버넌스, 정책 또는 인증 절차를 대체하지 않습니다. 다만 ISMS-P의 여러 통제 영역에 대해 기술적 집행과 증적(증거) 생성에 필요한 지원을 제공합니다.

BeyondTrust

TABLE OF CONTENTS

요약

한국의 조직(특히 규제가 엄격한 산업 분야의 많은 조직)은 ISMS-P, PIPA, CIUPA, 전자금융거래법(EFTA) 등 다양한 프레임워크의 적용을 받습니다. 이들 프레임워크는 접근 통제, 책임성, 운영 복원력에 대해 서로 중첩되면서도 상호 보완적인 요구사항을 부과합니다.

최근의 규제 조치와 사고 이후 점검 결과는 한 가지 사실을 분명히 보여줍니다. 인증을 받은 조직에서 발생하는 보안 실패는 정책의 부재보다는 접근 통제 및 권한(특권) 관리의 취약점에서 비롯되는 경우가 점점 더 많습니다.

본 가이드는 BeyondTrust의 '권한(특권) 중심' ID 보안 역량이 고위험 ISMS-P 통제 영역의 기술적 집행을 어떻게 지원하는지, 특히 한국의 규제 산업에서 감독이 강화되고 있는 영역을 중심으로 설명합니다.

소개

ISMS-P 준수(컴플라이언스) 프레임워크란?

정보보호 관리체계–개인정보(ISMS-P)는 민감 데이터를 처리하는 조직을 대상으로 하는 대한민국의 국가 인증 프레임워크로, 정보보호 요구사항과 개인정보 보호 요구사항을 하나의 통합 표준으로 결합합니다. 한국인터넷진흥원(KISA)이 운영·관리하며, 조직이 위험을 체계적으로 관리하고 개인정보를 보호하며 지속적인 준수를 입증할 수 있도록 설계된 포괄적인 통제 항목을 제시합니다.

ISMS-P는 일회성 인증 획득에 그치지 않고, 조직이 거버넌스·기술 통제·운영 프로세스를 포괄하는 지속적이며 감사가 가능한 보안 프로그램을 구현하도록 요구합니다. 또한 경영진의 감독부터 일상적인 접근 관리에 이르기까지 조직 전반의 모든 수준에서 책임성을 강조하여, 개인정보가 적절히 수집·저장·처리·보호되도록 합니다.

한국 시장에서 사업을 운영하거나 서비스를 제공하는 조직에게 ISMS-P는 선택 사항이 아닌 필수 규제 요구사항입니다. 또한, 엄격한 규제 준수 및 관리 감독 체계와도 직접적으로 연계되어 있습니다.
ISMS-P 인증을 획득하고 지속적으로 유지하는 것은 조직의 성숙한 보안 수준을 입증할 뿐만 아니라, 데이터 유출 위험을 줄이고 고객 및 규제 기관과의 신뢰를 강화하는 데 중요한 역할을 합니다.

효과적인 ISMS-P 정책 프레임워크는 조직이 다음을 수행할 수 있도록 합니다:

- 정보보호와 개인정보 보호를 모두 포괄하는 거버넌스 체계를 수립
- 시스템과 ID(신원) 전반에 걸쳐 엄격한 접근 통제 및 최소 권한 원칙을 적용
- 수집부터 폐기까지 개인정보 전 생애주기 전반을 보호
- 문서화된 통제, 모니터링, 보고를 통해 감사 대응(준비) 상태를 유지
- 국내 규제 요구사항 및 집행 기준에 맞춰 보안 운영을 정렬
- 지속적인 관리와 검토를 통해 위험 태세를 상시 평가하고 개선

한국의 규제 환경: 법과 표준 전반에서 수렴하는 기대치

ISMS-P는 국내 인증 체계로 시작되었지만, 그 통제 목적(Control Intent)은 다음과 같은 글로벌 보안 요구사항 및 기준과도 높은 수준으로 부합합니다:

- 최소 권한(Least Privilege) 접근
- 관리자 및 원격 접근에 대한 강력한 통제
- 로깅 및 모니터링을 통한 책임성 확보
- 제3자 및 외주(아웃소싱) 접근에 대한 거버넌스

- 운영 복원력 및 사고 대응 준비 태세
- 관리자 및 원격 접근에 대한 강력한 통제

이러한 주제는 다음 전반에서 반복·강화됩니다:

- PIPA(개인정보 보호법)와 같은 개인정보(프라이버시) 관련 법률
- CIUPA와 같은 산업/부문별 데이터 보호 법률
- EFTA(전자금융거래법)와 같은 운영 복원력 프레임워크
- ISO/IEC 27001, NIST SP 800-53, 제로 트러스트(Zero Trust) 아키텍처 등 글로벌 표준

왜 ID(신원) 보안이 이제 이사회(경영진) 차원의 리스크인가

최근 한국의 사이버 사고 조사에서는 다음과 같은 문제가 반복적으로 지적되었습니다:

- 과도하거나 상시 유지되는 관리자 권한
- 공유되거나 거버넌스가 미흡한 특권(권한) 계정
- 협력사/외주 접근에 대한 취약한 통제
- 접근이 실제로 어떻게 집행되었는지에 대한 증적(증거)의 부족

그 결과 ISMS-P 요구사항을 충족하는 것, 특히 접근과 관련된 이러한 공통 취약점을 보완하는 통제 영역은 규제기관뿐 아니라 IT 보안 리더와 그 팀의 핵심 과제가 되었습니다.

CISO 관점에서 특권(권한) 접근은 리스크를 증폭시키는 요인이 되었습니다:

- 단 하나의 관리자 계정이 침해되면 여러 프레임워크와 법적 요구사항 전반의 준수가 무너질 수 있습니다.
- 권한 통제가 약하면 랜섬웨어, 내부자 위협, 공급망 공격의 피해 규모가 커집니다.
- 취약한 감사 추적(Audit Trail) 체계는 보안 이슈 발생 시 조사 및 대응 역량을 제한하며, 결과적으로 침해 사고에 따른 비용과 영향을 더욱 증가시킬 수 있습니다.

BeyondTrust의 역할(적용 영역)

BeyondTrust는 다음을 통해 조직이 규제 의도를 실제 운영 통제로 구현할 수 있도록 지원하는 '권한(특권) 중심' ID 보안 역량을 제공합니다:

최소 권한(Least Privilege) 원칙을 적용하여 공격 표면을 줄이고, 업무 수행에 필요한 최소 수준의 권한만 필요한 시간 동안 부여함으로써 공격 발생 시 영향 범위(Blast Radius) 또한 최소화할 수 있습니다. 이러한 접근 방식은 온프레미스, 클라우드, Windows, macOS, Unix/Linux 환경 전반에 걸쳐 적용 가능합니다.

자격 증명을 노출하지 않고 원격 및 관리자 접근을 안전하게 보호합니다.
원격 근무자, 외부 협력업체, IT 및 OT 환경 등 다양한 환경에서 BeyondTrust는 취약한 VPN을 대체할 수 있는 완전한 감사 추적 기반의 안전한 원격 접근 환경을 제공합니다.

감사 및 조사에 적합한 상세 증적을 제공합니다.
누가 특정 자격 증명이나 시스템에 접근했는지, 언제 어떤 작업을 수행했는지에 대한 추적은 물론, IT 환경 전반의 보안 리스크 현황까지 가시화하여 감사 대응 및 경영진 보고에 필요한 정보를 제공합니다.

이러한 역량은 감독과 점검이 특히 강화되는 ISMS-P 핵심 통제 영역과 강하게 정렬됩니다.

핵심 ISMS-P 통제 영역과 BeyondTrust 정렬

다음 섹션에서는 ISMS-P의 핵심 통제 영역과 그 중요성, 그리고 BeyondTrust 솔루션을 활용해 조직이 해당 통제에 어떻게 정렬(부합)할 수 있는지 설명합니다.

인증 및 권한 부여 관리 (ISMS-P 2.5)

CISO 관점

ISMS-P는 특권(권한) 계정 및 관리자 계정이 생성·사용·검토·회수(폐기)되는 방식에 큰 비중을 둡니다. 특히 고객 데이터 또는 금융 데이터 시스템에 접근 가능한 관리자 계정은 중점 관리 대상입니다.

BeyondTrust 지원 방식

- Endpoint Privilege Management는 엔드포인트와 서버에서 상시 관리자 권한(standing admin rights)을 줄입니다.
- 권한은 승인된 애플리케이션 또는 작업에 대해 필요할 때만 부여됩니다.
- 특권 계정 및 아이덴티티에 대한 가시성 확보는 정기적인 접근 권한 검토(Access Review)를 효과적으로 지원합니다.

규제 관련성

- 특권(권한) 계정 통제에 대한 ISMS-P 요구사항을 지원합니다.
- 접근 권한을 최소화하라는 PIPA의 기대치(원칙)와 정렬됩니다.
- 신용정보를 처리할 수 있는 주체를 제한함으로써 CIUPA 관련 노출(리스크)을 줄이는 데 도움이 될 수 있습니다.

접근통제 및 원격 접근 (ISMS-P 2.6)

CISO 관점

원격 및 관리자 접근 경로는 공격자에 의해 자주 악용되기 때문에 점점 더 운영 리스크로 간주됩니다. 전통적으로 원격 접근은 VPN을 중심으로(원격 데스크톱 서비스 등과 함께) 제공되어 왔지만, 대부분의 경우 특권(권한) 접근에는 적합하지 않은 것으로 드러났습니다.

ISMS-P는 시스템, 애플리케이션, 데이터베이스, 원격 인터페이스에 대한 접근을 명확히 정의하고 제한하며 집행할 것을 요구합니다. 특히 관리자 및 원격 접근에 대해서는 보다 엄격한 통제가 요구됩니다.

BeyondTrust 지원 방식

- Privileged Remote Access는 자격 증명 주입(credential injection)을 활용해 비밀번호나 시크릿을 사용자에게 노출하지 않고도 접근을 부여하면서, 중요 시스템에 대해 ID 기반 최소 권한 접근을 강제합니다.
- 모든 원격 세션은 완전하게 모니터링·기록되며 감사가 가능합니다. 또한 정책 기반 통제를 통해 누가 어떤 리소스에 언제 접근할 수 있는지 관리합니다.
- 세분화된 접근 통제와 JIT(Just-in-Time) 권한 집행을 통해 상시 권한을 제한하고, 시스템 간 횡적 이동(lateral movement) 위험을 줄입니다.

규제 관련성

- ISMS-P의 접근통제 요구사항을 충족하는 데 기여합니다.
- 비인가 시스템 접근을 방지하라는 EFTA의 기대치(요구사항)를 지원합니다.
- 개인정보를 처리하는 시스템에 대한 PIPA 통제를 강화합니다.

외부 당사자 및 공급업체(벤더) 보안 (ISMS-P 2.3)

CISO 관점

제3자 접근은 보안 사고의 가장 흔한 근본 원인 중 하나로 남아 있으며, 감사 지적사항 및 시정조치(리메디에이션) 요구의 주요 초점이 되곤 합니다.

많은 조직이 외부 협력업체(Third-Party)에 안전한 접근 권한을 제공하면서도, 사용자 권한을 세밀하게 통제하는 데 어려움을 겪고 있습니다.

특히 계약업체가 관여된 환경에서는 공유 계정 사용으로 인해 자격 증명이 사용자에게 노출되는 문제가 발생할 수 있으며, 이는 추가적인 보안 리스크로 이어질 수 있습니다

ISMS-P는 조직이 외부 접근을 식별하고, 계약상 보안 요구사항을 강제하며, 준수 여부를 점검하고, 계약 종료 시 접근을 반드시 종료(차단)하도록 요구합니다.

BeyondTrust 지원 방식

- Privileged Remote Access는 공유 계정 없이도, 제한된 시간 동안 특정 작업에 필요한 외부 협력업체 접근 권한을 안전하게 제공합니다.
- 작업 완료 또는 계약 종료 시 접근을 자동으로 회수(차단)합니다.
- 세션 기록은 벤더 활동에 대한 증적(증거)을 제공합니다.

규제 관련성

- ISMS-P의 외부 당사자(외부자) 통제 요구를 직접적으로 지원합니다.
- 위탁(아웃소싱) 처리에 대한 CIUPA 및 PIPA 의무와 정렬됩니다.
- EFTA 관점의 시스템적 리스크를 줄이는 데 기여합니다.

로깅, 모니터링 및 사고 증적 (ISMS-P 2.9 / 2.10 / 2.11)

CISO 관점

보안 사고 대응 시 이상 징후를 탐지하고, 임직원·승인된 제3자 또는 공격자의 행위를 검토할 수 있는 능력은 무엇보다 중요합니다.

또한, 사이버 보안 리더는 조직의 위험 수용 수준(Risk Appetite)을 고려하면서도, 어떤 리스크를 우선적으로 대응해야 하는지에 대해 사실 기반으로 설명할 수 있어야 합니다.

특히 동종 업계에서 보안 사고가 발생했을 경우, 우리 조직 또한 유사한 공격 방식의 영향을 받을 가능성이 있는지에 대해 경영진 및 이사회의 질문에 대응할 수 있는 역량이 점점 더 중요해지고 있습니다.

ISMS-P는 로그를 보호하고 검토하며, 오남용·이상 행위·보안 사고를 탐지하는 데 활용할 것을 요구합니다.

BeyondTrust 지원 방식

- 엔드포인트 및 서버에서의 특권(권한) 활동을 로깅합니다.
- 조사(포렌식)를 위해 원격 특권 세션을 기록할 수 있습니다.
- Hidden Paths to Privilege™를 식별하고, 사람·비인간(NHI)·AI를 포함한 모든 ID 전반에 걸쳐 권장 시정조치(리메디에이션)를 제시할 수 있습니다.
- SIEM 도구와의 연동을 통해 이상 행위 분석을 지원합니다.

규제 관련성

- ISMS-P의 로깅 및 모니터링 통제를 지원합니다.
- 개인정보 접근에 대한 모니터링을 강조하는 PIPA 가이드라인과 정렬됩니다.
- EFTA 사고 점검(사후 리뷰)에 대비한 포렌식 준비태세를 강화합니다.

규제 관련성

- ISMS-P의 외부 당사자(외부자) 통제 요구를 직접적으로 지원합니다.
- 위탁(아웃소싱) 처리에 대한 CIUPA 및 PIPA 의무와 정렬됩니다.
- EFTA 관점의 시스템적 리스크를 줄이는 데 기여합니다.

보유 중인 개인정보 보호 (ISMS-P 3.2)

조직이 보유하는 개인정보의 범위가 넓고 최근 데이터 유출 사고가 이어지면서, 규제기관이 이 민감 정보에 대한 접근을 조직이 어떻게 보호하는지에 그 어느 때보다 집중하는 것은 당연한 흐름입니다.

ISMS-P는 개인정보를 보유·이용하는 경우 보호조치를 요구하며, 목적 및 필요성에 근거한 접근 제한을 포함합니다.

BeyondTrust 지원 방식

- 민감한 시스템에 대한 관리자 접근 시 최소 권한 원칙을 적용 및 강제합니다.
- 특권 접근이 필요한 경우 세션 단위 감사로 책임성을 확보합니다.

경영진 핵심 요약

ISMS-P 및 유사한 보안 프레임워크는 더 이상 단순 문서 중심의 인증 체계가 아닙니다.
특히 특권 접근 관리 영역에서는 실제 운영 통제의 효과성을 검증하는 체계로 변화하고 있습니다.

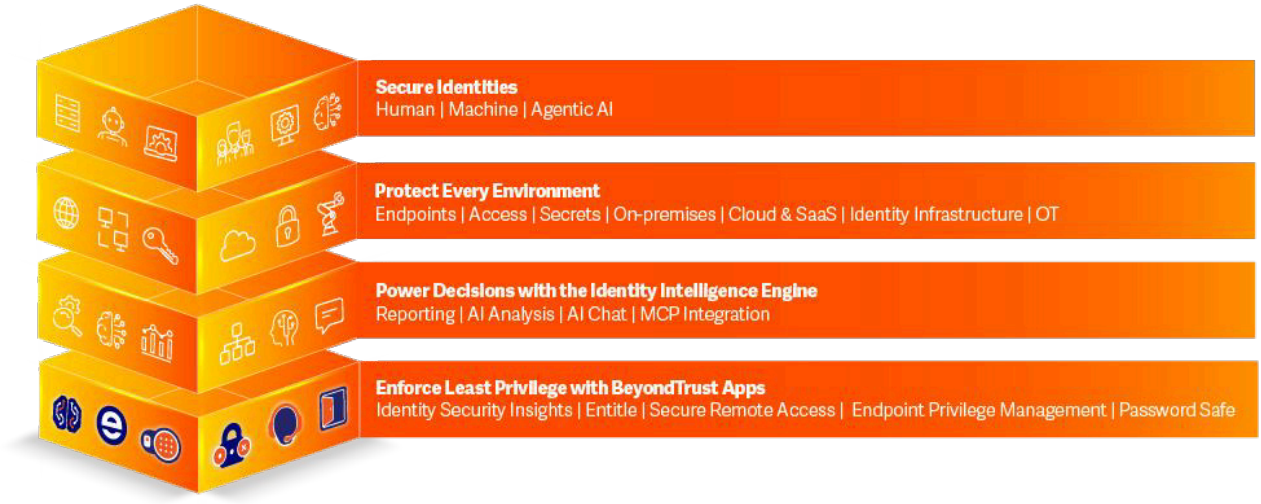
BeyondTrust는 다음과 같은 요구가 특히 강하게 제기되는 영역에서 가장 높은 정합성을 보입니다:

- 특권(권한)은 실시간으로 최소화되어야 함
- 접근 결정은 '가정'이 아니라 '집행'되어야 함
- 증적은 상세하고, 시스템이 생성하며, 검토 가능해야 함
- 관리자 및 제3자 활동은 사후에 재구성(추적) 가능해야 함

ISMS-P × BeyondTrust Control Mapping

ISMS-P 통제 영역	리스크 초점	BeyondTrust 지원 가능 영역
2.5 인증 및 권한부여	과도한 / 상시 특권(권한)	ID 기반 원격접근, 애플리케이션 단위 권한 통제
2.6 접근통제	비인가 시스템 및 원격 접근	ID 기반 원격접근, 애플리케이션 단위 권한 통제
2.3 외부 당사자 보안	벤더 및 위탁(외주) 접근 리스크	시간 제한 최소 권한 벤더 접근, 세션 감사
2.9 로그 관리	감사 증적 부족	특권 활동 로깅 및 숨은 권한 상승 경로 식별
2.10 시스템 보안관리	관리자 오남용, 횡적 이동	권한 격리 및 세션 통제
2.11 사고 대응	제한된 포렌식 역량	세션 기록 및 조사 지원
3.2 개인정보 이용	개인정보 시스템 과다 노출	민감 정보 및 시스템에 대한 관리자 접근 제한

BeyondTrust Pathfinder 플랫폼



BeyondTrust는 권한 중심(Privilege-centric) 아이덴티티 보안 분야의 글로벌 리더로서, 조직이 전체 아이덴티티 공격 표면(Identity Attack Surface)을 가장 효과적으로 관리하고, 외부 공격 또는 내부자에 의한 위협 등 어떠한 형태의 위협도 무력화할 수 있도록 지원합니다.

BeyondTrust는 권한 중심(Privilege-centric) 아이덴티티 보안 분야의 글로벌 리더로서, 조직이 전체 아이덴티티 공격 표면(Identity Attack Surface)을 가장 효과적으로 관리하고, 외부 공격 또는 내부자에 의한 위협 등 어떠한 형태의 위협도 무력화할 수 있도록 지원합니다.

Identity Security Insights® – 인간 및 비인간 아이덴티티, 권한, 접근 경로를 지속적으로 분석하여 아이덴티티 리스크에 대한 통합 가시성을 제공함으로써 숨겨진 위험을 드러내고, 선제적 위협 탐지를 가능하게 합니다.

Password Safe® – 모든 특권 계정 및 특권 자격 증명(비밀번호, 시크릿, 키 등)의 자동 검색, 온보딩, 관리 및 감사 기능을 제공합니다.

Privileged Remote Access – 클라우드, 온프레미스 및 OT 환경에 대해 안전한 적시(Just-in-Time) 원격 접근을 제공하며, 아이덴티티 기반 제어, 자격 증명 주입, 세션 감사 기능을 통해 기존 VPN에 의존하지 않고도 보안을 강화합니다.

Endpoint Privilege Management – 최소 권한(Least Privilege) 적용과 애플리케이션 제어를 결합하여 Windows, macOS, Unix 및 Linux 시스템 전반에서 관리자 권한을 관리하고 축소합니다. 승인된 애플리케이션과 작업만 상승된 권한으로 실행되도록 보장하면서도, 사용자 생산성과 보안 컴플라이언스를 유지합니다.

Entitle – 상시(always-on) 접근을 제거하고 적시(Just-in-Time, JIT) 자동화로 대체함으로써 권한 공격 경로를 차단하고, 팀의 업무 속도를 저해하지 않으면서도 위험을 줄입니다.

Remote Support – 서비스 데스크 기술자가 어디서든 모든 사용자 또는 디바이스를 지원할 수 있도록 하며, 강화된 보안을 동시에 보장합니다. 직원, 벤더 및 서비스 데스크에서 필요한 모든 원격 접근에 최소 권한과 강력한 감사 통제를 적용합니다.

Active Directory Bridge – Microsoft Active Directory 인증, SSO 및 정책 통제를 Unix 및 Linux 시스템까지 확장하여, 중앙 집중식 아이덴티티 관리와 일관된 접근 통제, 감사 및 컴플라이언스를 혼합 운영체제 환경 전반에서 구현할 수 있도록 지원합니다.

다음 단계

본 가이드를 통해 추가적인 문의 사항이 생기셨거나, BeyondTrust의 특권 중심(Privilege-Centric) 아이덴티티 보안 솔루션에 대해 더 자세한 정보를 원하신다면 언제든지 한국 담당 팀으로 문의해 주시기 바랍니다.

BeyondTrust는 다양한 조직의 컴플라이언스 대응 및 보안 강화 활동을 지속적으로 지원하고 있습니다. 또한 BeyondTrust 솔루션에 대해 더 자세히 확인하고 싶으시다면, 아래 자료들도 함께 참고해 주시기 바랍니다.

- Privileged Access Management (PAM) Buyer's Guide & Checklist
- Mapping BeyondTrust Capabilities to NIST Zero Trust (SP 800-207)
- PAM Maturity Model Guide
- Guide to Identity Security Defense-in-Depth
- Gartner® Research: How to Secure Enterprise Agentic AI Ambition

무료 Identity Security Risk Assessment 받기

무료로 제공되는 BeyondTrust의 수상 경력 기반 아이덴티티 보안 위험 평가 서비스를 신청해보세요.

클라우드 및 온프레미스 환경, SaaS 애플리케이션, 사람 및 비인간 아이덴티티(NHI), 그리고 AI 에이전트 전반에 숨어 있는 **Paths to Privilege™**를 식별하여, 조직의 아이덴티티 공격 표면에 대한 초기 가시성을 빠르게 확보할 수 있습니다.

이를 통해 아이덴티티 인프라의 주요 보안 현황을 파악하고, 보안 의사결정 및 감사 대응 체계(Audit Readiness) 강화를 지원하는 초기 분석 결과를 제공받을 수 있습니다. 또한, 활성화된 권한 오남용에 대해 30일간 지속 모니터링 기능도 함께 제공됩니다.
지금 시작해보세요.

>>> BeyondTrust 소개

BeyondTrust는 Paths to Privilege™를 보호하는 글로벌 특권 중심(Privilege-centric) 아이덴티티 보안 분야의 선도 기업입니다. BeyondTrust의 아이덴티티 중심 접근 방식은 특권과 접근을 보호하는 수준을 넘어, 조직이 전체 아이덴티티 공격 표면(Identity Attack Surface)을 효과적으로 관리하고 외부 공격이나 내부자에 의한 위협을 포함한 다양한 위협을 무력화할 수 있도록 지원합니다.

BeyondTrust는 침해를 예방하고 공격의 피해 범위(Blast Radius)를 최소화하는 아이덴티티 보안 혁신을 주도하는 동시에, 더 뛰어난 고객 경험과 운영 효율성을 제공합니다. BeyondTrust는 포춘 100대 기업 중 75개 기업을 포함한 20,000개 고객과 전 세계 파트너 에코시스템으로부터 신뢰받고 있습니다.

원하시면 더 자연스러운 마케팅 톤(한국어 웹/브로셔 스타일), 또는 더 기술적인 톤(보안 담당자용)으로도 다듬어 드릴게요.

Learn more at **www.beyondtrust.com.**