Norton 제품 및 서비스 개인정보 취급방침 – *2018 년 11 월 7 일 마지막 업데이트*

본 취급방침은 반드시 읽어야 하고, Symantec – Norton 개인정보 보호정책과 함께, 이에 추가하여 적용됩니다. 이는 Norton 제품 및 서비스에 의해 수집된 데이터의 범주, 그리고 이러한 데이터 범주를 처리하는 목적에 대해 설명합니다. 이는 데이터 주체로서의 개별 Norton 사용자, 그리고 데이터 컨트롤러로서의 중소 기업의 Norton 사용자 모두에게 필수 투명성 정보를 제공하기 위해 고안되었습니다. 별표(*)로 표시된 데이터 범주는 해당 Norton 제품 기능 및 서비스 기능을 전달하기 위한 목적으로 Symantec 으로 전송되는 개인 데이터라는 점에 유의하십시오. 기타 모든 데이터 범주는 식별 가능하지 않은 형태로 처리하기 위한 목적으로 Norton 소프트웨어에 의해 수집됩니다.

모든 Norton 의 제품과 서비스는 Symantec – Norton 글로벌 개인정보 보호정책에 명시된 최고 표준을 준수합니다. 또한 제품 또는 서비스에 관한 설명 이외에, 각 Norton 제품과 서비스의 고유한 특징과 구체적인 용도에 관해 투명하게 밝히기 위해, 본 취급방침은 당사가 수집하는 개인 데이터, 개인 데이터를 처리하는 용도에 관해 설명합니다.

귀하가 본 취급방침의 일체의 일부분 또는 측면을 수락할 수 없는 경우, 해당 제품, 서비스 또는 그 기능을 다운로드, 설치 또는 달리 사용하지 말고 또한/또는 문제의 제품, 서비스 또는 기능을 즉시 제거하거나 사용을 중단하십시오. 제품과 서비스 기능이 기능의 다운로드, 설치, 활성화 또는 사용 시 귀하에게 추가 개인 데이터 제공을 요구하거나, 제품 또는 서비스의 특정 선택적 기능으로부터 혜택을 받기 위해 필요한 개인 데이터 처리에 대한 동의를 요구하는 경우, 충분한 정보에 입각한 구체적인 동의를 제공할 수 있도록 귀하에게 본 취급방침의 검토를 요청드릴 것입니다.

목차

Norton App Lock

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton App Lock 은 사용자가 핀, 암호 또는 잠금 패턴을 사용하여 모바일 애플리케이션을 보호할 수 있게 해줍니다. 모바일 기기를 분실 또는 도난당하는 경우, 기기의 전면 카메라(구비되어 있는 경우)가 기기 잠금 해제에 3 번 실패한 후 사진을 촬영하도록 App Lock 을 구성할 수 있습니다.	*1. 사용자의 이메일 주소 2. 사용자 설정 PIN, 모바일 애플리케이션을 위한 암호 3. 사용자의 선택에 따른, 설정에 기초한 사진	1. 사용자의 이메일 주소는 Norton App Lock 암호 복구와 재설정을 처리할 수 있도록 수집하여 Symantec 에 전송합니다. 2. 3. 제품이 사용자 입력정보로부터 수집하는 모든 다른 데이터는 사용자의 기기에 저장됩니다.

Norton Clean

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Clean 은 스토리지 최적화 기능으로, 사용자의 모바일 기기 메모리 캐시를 청소하여 광고와 원하지 않은 데이터를 삭제하고 추가 스토리지 공간을 확보합니다.	모바일 기기의 고유한 기기 식별자(IMEI)	IMEI 번호는 기기로부터 수집하여 Symantec 에 전송합니다. 전송 후 IMEI 번호는 즉시 일체의 추가 처리 전 해시됩니다. 해시는 제품의 고유한 사용을 모니터링하기 위해 처리됩니다. 데이터가 해시된 후, 원래 기기로 이를 역추적할 수 없기에, 사용자와 기기 자체를 추적 또는 모니터링할 수 없습니다.

Norton Error Management

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Error Management 는 Norton 제품 사용 시 경험하는 문제들을 문서화합니다. 이러한 경우, 사용자는 Symantec 에 오류를 보고하기로 선택할 수 있습니다.	1. 컴퓨터 상태 정보(시스템 언어, 국가 로캘, 운영 체제 버전) 2. 처리 실행, 그 상태, 성능 정보 3. Norton 제품이 문제를 경험했을 당시 열려 있던 파일과 폴더로부터의 데이터	1.-2.-3. 시스템 정보는 Symantec 이 발생한 문제를 정정하고 Norton 제품의 성능을 개선하기 위해 처리합니다. 일부의 경우, 보안 위협 또는 취약성으로 인해 오류가 발생하는 경우, Symantec 은 일부 비-사용자별, 또는 비-신원 확인 데이터를 추출하여 연구소, 다른 보안 소프트웨어 벤더와 같은 보다 광범위한 사이버 보안 커뮤니티 파트너들과 공유할 수 있습니다. 이러한 공유의 목적은 위험 인식, 탐지, 예방을 증진하기 위한 것입니다. Symantec 은 또한 이러한 정보로부터 추출한 통계를 사용하여 보안 위험 동향을 추적하고 이에 관한 보고서를 발표할 수 있습니다.

Norton Community Watch

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Community Watch 는 Norton 보안 제품 사용자들이 새로운 보안 위협에 대한 식별을 개선시키고 이에 대한 보호를 제공하는 시간을 단축시킬 수 있게 해줍니다. 프로그램은 선별 보안과 애플리케이션 데이터를 수집하고, 새로운 위협과 그 출처를 파악하는 분석을 위해 Symantec 에 데이터를 제출합니다. 프로그램은 사용자로부터 전송된 데이터를 분석하여 보다 효과적이고 견실한 보안 제품 개발을 돕습니다. Norton Community Watch 프로그램에 가입함으로써: 1. 귀하는 귀하와 다른 참여자들이 제출하는 데이터를 통해 사이버 위협에 관한 보다 효과적이고 견실한 지식, 이에 대한 보호 수단을 개발하는 데 참여하게 됩니다. 당사의 백엔드 기술은 귀하 또는 일체의 다른 개인에게 영향을 미칠 일체의 결정을 내림이 없이, 고급 알고리즘을 사용하여 기계에 다운로드, 설치 또는 실행하는 각 파일의 보안 평판 등급을 계산합니다. Norton 보안 제품 사용자들은 Norton 제품이 다음을 실행할 때 이 새로운 혁신적인 기술의 혜택을 받게 됩니다. *a. Download Insight 로 해로운 다운로드를 차단할 때. Norton 은 다운로드가 안전한 또는 위험한 것으로 알려져 있는지 또는 미상의 보안 프로필이 있는지 알려줍니다. 다운로드가 안전하지 않은 경우, 당사 제품은 귀하를 보호하기 위한 즉각적인 조치를 취합니다. b. 개선된 탐지율을 제공하고 위양성을 감소시킬 때, *c. 제출 후 분석하고 Norton Community Watch 를 통해 유효한 것으로 확인된 파일들을 보다 신속하게 제거함으로써 Norton Insight 를 사용하여 보다 신속한 스캔을 실행할 때. 2. 중요한 보안과 애플리케이션 데이터를 제공함으로써, 귀하는 새로운 위협을 식별하고 이들이 추가로 확산되기 전 차단하는 데 필요한 인텔리전스에 기여하게 됩니다. *Norton Insight 는 Windows OS 에서만 사용할 수 있습니다.	1. 기계 ID(Symantec 이 생성한 데이터) 2. 제품 일련 번호(Symantec 이 제품에 배정한 데이터) 3. Norton 계정 번호(Symantec 이 생성한 데이터) *4. 파일 경로 *5. 멀웨어로 확인된 실행 불가하고 이식 가능한 실행 파일 6. Norton 제품이 사기적일 수 있다고 간주하는 방문한 웹사이트의 URL 7. 사용자가 컴퓨터에 다운로드한 보안 위험을 설치하기 전 가장 최근 방문한 웹사이트의 URL 8. 잠재적인 보안 위반이 발생한 시간을 포함한 때때로 사용자의 기기에서 실행하는 프로세스와 애플리케이션에 관한 정보 9. 잠재적인 보안 위협에 대응하여 사용자의 기기가 전송한 데이터 샘플	Norton Community Watch 는 Symantec 이 백엔드에 호스트하고 관리하는 서비스이기에, 수집하는 모든 데이터는 다음과 같이 Symantec 으로 전송됩니다. 1. 기계 ID 는 라이선스 권리와 권한을 감사하고 집행하기 위해 각 구독 제품을 사용하는 고유한 기기 수를 추적하는 데 필요합니다. 2. 제품 일련 번호는 각 사용자에게 제공되고, Symantec 이 각 제품의 사용을 허가했는지 확인하는 데 사용됩니다. 3. Norton 계정 번호는 특정 Norton 제품을 구독하는 사용자 수를 추적하는 데 사용됩니다. 4.-5. 파일 경로와 실행 불가하고 이식 가능한 실행 파일은 사용자의 기기에 영향을 미치거나 기기로부터 배포되는 사이버 위협의 기원과 논리적 위치 파악을 돕기 위해 수집합니다. 6.-7. URL 은 잠재적인 보안 위험의 웹 기반 출처를 파악하고, 악의적인 행동, 유해한 사건, 사기성 웹사이트, 크라임웨어, 다른 형태의 인터넷 보안 위협을 탐지할 수 있는 Symantec 제품과 서비스의 능력을 개선하는 데 사용됩니다. 8.-9. 기기 데이터는 사이버 위협에 대한 Symantec 의 지식과 이해를 개선하는 데 사용됩니다. 기기 데이터는 또한 미래의 Symantec 제품과 서비스 사용자들에게 보다 효과적인 보호를 제공하고, 사이버 보안 동향의 통계 분석을 위해 처리됩니다.

Norton Core

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Core 는 라우터에 연결된 기기에 멀웨어, 바이러스, 해커, 다른 사이버 위협에 대한 보호를 제공하는 무선 라우터입니다.	*1. 무선 네트워크 SSID/암호(암호화) 2. 기기에 이름을 지정할 때 사용자가 포함시키는 일체의 개인 데이터, 사용자가 제공한 경우 기기를 배정받는 개인의 이름 또는 별명, 기기 사용자 에이전트 데이터/앱 사용자 에이전트 데이터(기기 유형, 제조업체, 모델, 운영 체제, IP 주소 포함)를 포함한 기기 정보 3. 마지막 기기 사용 시간, 각 연결된 기기의 인터넷 사용 시간, 네트워크 연결의 게이트웨이 로그에 관한 데이터를 포함한 기기 사용에 관한 데이터 4. 차단된 웹사이트, 방문한 웹사이트, 시간과 콘텐츠 필터 정보, 위험한 것으로 결정 또는 간주된 웹사이트의 URL 을 포함한 사용자가 정의하고 구성한 보호자 통제 정보와 설정 *5. 사용자가 Norton 계정을 만들기 위해 제공할 수 있는 개인 데이터(예: 사용자 이름, 선택적인 사진) *6. 사용자 ID, 이름, 역할, 사용자 특이 정책, 기기 정보와 같은 고객 지원과 연결 지원을 위해 사용자가 제공하는 개인 데이터 7. 악성 실행 파일/모바일 앱의 다운로드 시도 로그, 다른 위험한 사건 또는 행동 기록, 멀웨어 샘플과 같은 아티팩트를 포함한 사이버 위협 원격 분석 *8. 사용자 연락처 정보, 표현된 기본 설정 *9. 배송 주소, 관련 정보 10. Norton Core 는 Norton Community Watch 에 참여할 수 있게 해줍니다.	1. 네트워크 정보는 와이파이 네트워크의 사용자 정의 구성을 위해 처리합니다. 2. 기기 정보는 라이선스를 관리하고, 라우터의 상태와 연결을 모니터링하고 이의 디버깅을 지원하기 위해 기기와 그 트래픽을 분석하며, 제품 사용을 이해하고 경고에 대응하기 위해 처리합니다. 3. 기기 사용 현황 데이터는 다음을 위해 처리합니다. • Norton Core 의 성능을 최적화하기 위한 목적, • 사용자들에게 사이트 안전에 관해 알리기 위한 목적, 그리고 • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적. 4. 보호자 통제 정보와 설정은 사용자가 통제 프로필에 정의한 규칙과 정책을 집행하고, 사용자가 이러한 프로필과 관련된 개인 데이터 오용을 탐지하도록 돕고, 사용자/통제 프로필과 소통하는 데 사용됩니다. 5.-6. 사용자 계정 정보는 Symantec 이 고객 계약에 약술된 서비스를 이행하고 기술 지원을 제공하기 위해 수집합니다. 7. 사이버 위협 원격 분석은 Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발 목적으로 Symantec 에 전송됩니다. 8. 사용자 연락처 정보와 기본 설정은 다음을 위해 Symantec 에 전송합니다. • Norton Core 의 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 사용자에게 사용자 경험을 개선할 방법을 알리기 위한 목적, • 사용자의 기본 설정(예: 언어, 지리적 지역)에 기반하여 사용자에게 제공하는 정보를 맞춤화하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 9. 배송 주소 및 관련 정보는 Norton Core 하드웨어를 사용자에게 배송하기 위해 처리합니다. 10. Norton Community Watch 관련 정보에 관한 추가 상세정보는 본 취급방침의 Norton Community Watch 섹션을 참조하십시오. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고

		• 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton Mobile Security

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Mobile Security 는 구독자가 보호하기로 선택하는 보호 대상 사용자와 그 기기에 디지털 위협으로부터 스마트폰과 태블릿 보호, 분실 또는 도난당한 기기 회수, 연락처 정보 복원을 제공합니다.	1. 장비 식별자(예: IMEI, WiFi MAC 주소, UDID), 구독자 정보, 휴대폰 번호와 기타 보호 대상 사용자 연락처 정보, 기기 이름/유형과 제조업체, 운영 체제 유형과 버전, 무선 이동통신업체, 네트워크 유형, 원산지, 지원 케이스 ID, 사용자 설치 인증서, 기기로부터의 웹사이트 도메인 이름과 관련 SSL 인증서 체인, IP 주소를 포함한 보호 대상 사용자의 모바일 기기 데이터 2. 다운로드와 사용 빈도 정보, 로그 데이터와 쿠키, 사용자가 네트워크 서비스에 연결하는 방법에 관한 네트워크 서비스 정보와 같은 사용 현황 데이터 3. 사용자를 멀웨어 또는 위험한 기능으로부터 보호해 주는 것으로 알려진 Symantec 앱 데이터베이스에 현재 포함되어 있지 않은 스캔한 앱, 캘린더, 이용 가능한 경우 SD 카드 콘텐츠를 포함한 제품이 스캔을 실시할 때마다 사용자 기기 내 파일과 애플리케이션 이름 4. 웹 검색 URL, 기록, 책갈피 *5. 사용자 선택에 따라, 전화, SMS 로그를 포함한 사용자 기기의 연락처 6. 전화 통화, 기기 오디오 설정 *7. 기기 위치 데이터	1. 모바일 기기 데이터, 구독자 정보, 보호 대상 사용자 연락처 정보는 다음을 위해 처리합니다. • 제품 성능을 활성화하고 최적화하기 위한 목적, • Symantec 을 위해 보호 대상 사용자의 신원을 인증하기 위한 목적, • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 서비스 제공을 위해 보호 대상 사용자와 소통하기 위한 목적, • 라이선스 관리를 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 사용 현황 데이터는 다음을 위해 처리합니다. 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적. 3. 파일, 애플리케이션 이름, 캘린더(예: 초대 내 URLS), SD 카드 콘텐츠는 다음을 위해 처리합니다. • 사용자에게 잠재적으로 해로운 애플리케이션을 경고하기 위한 목적, • 멀웨어가 있는지 기기를 스캔하기 위한 목적, • 사용자가 제품의 초기화 명령을 활성화하고 실행하기로 선택하는 경우 기기로부터 개인 콘텐츠를 지우기 위한 목적. 4. 검색 데이터는 다음을 위해 처리합니다. • 사용자들에게 사이트 안전에 관해 알리기 위한 목적, • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적, 그리고 • 사용자가 제품의 웹 보호 기능 또는 초기화 명령을 사용하기로 선택하는 경우 검색 기록과 책갈피를 지우기 위한 목적. 5. 사용자 기기의 전화와 SMS 로그를 포함한 연락처는 사용자가 사용하기로 선택하는 경우 통화/문자 차단 기능을 제공하기 위해 처리합니다. 6. 사용자가 제품의 차단 기능 및/또는 스크림 명령을 활성화하고 사용하기로 선택하는 경우, 전화 설정은 연락처로부터 걸려온 전화를 차단하거나 기기의 오디오 설정을 수정하는 데 사용됩니다. 7. 8. 기기 위치와 사진 데이터는 사용자의 기기를 분실 또는 도난당하는 경우 이를 찾기 위해 보호 대상 사용자의 요청 시 수집할 수 있습니다. 제품은 또한 보호 대상 사용자의 기기를 분실 또는 도난당하는 경우 이를 찾기 위해 구독자에게 원격 명령을 제공할 수 있습니다. 일부의 경우에 기기가 분실 또는 도난당한 것으로 보고되는 경우, 원격으로 기기를 잠글 것입니다. 또는 기기가 분실 또는 도난당한 것으로 보고되는 경우, 언제든 제품을 종료할 수 있습니다. 보호 대상 사용자의 허가 시, 제품이 현재 사용되고 있지 않은 경우에도 보호 대상 사용자가 기기의 최근 이동을 추적할 수 있도록 기기의 마지막으로 알려진 최대 10개의 위치 기록을 보관할 수 있습니다.

	*8. 또한 기기의 전면 카메라가 구비되어 있고 기기가 분실 또는 도난당한 것으로 보고되는 경우, 기기가 계속하여 사용될 때, 기기의 잠금 해제에 1 번 실패한 후 부정확한 암호를 입력하는 경우, 또는 기기의 전원을 끈 후 다시 켜는 경우, 기기의 전면 카메라가 사진을 촬영하도록 제품을 구성할 수 있습니다. 9. 연락처, 통화 기록, 전화와 문자 메시지를 포함한 모바일 기기의 데이터 백업 사본	9. 백업 데이터는 사용자가 사용하기로 선택하는 경우 제품의 백업과 복구 기능을 제공하기 위해 처리합니다. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton Security Scan

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Secure Scan 은 사용자가 선택한 끝점 기기(들)의 스캔을 제공하고, 잠재적인 문제 또는 위험을 식별할 것이며, 사용자에게 제품과 솔루션을 추천할 것입니다.	1. 기계 ID(Symantec 이 내부적으로 생성한 데이터), 기기의 설치/제거 기능, 기기 정보와 기기 사용자 에이전트 데이터/앱 사용자 에이전트 데이터(기기 유형, OS 버전, OS 언어, 제조업체, 모델, 운영 체제, 관련 지리적 정보 등) 2. 스캔한 파일, 사용자 경험, 발견/교정/남은 위협에 관한 원격 분석 정보, 제출 후 스캔 날짜와 시간, 파일 경로 또는 폴더 이름에 포함되어 있는 경우, 우발적으로 개인 데이터를 포함할 수 있는 설치와 운영에 관한 상태 정보	1. 기계 ID 및 관련 정보는 Symantec 이 다음 용도로 사용합니다. • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 서비스 제공을 위해 사용자와 소통하기 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 서비스 사용과 기본 설정을 이해하기 위한 목적. 2. 원격 분석 정보는 Symantec 이 다음 용도로 사용합니다. • 서비스 이행을 활성화하고 최적화하기 위한 목적, 그리고 • Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton Secure Login

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Secure Login(NSL)은 사용자들을 인증하는 간단하고 안전하며 중앙화된 방식을 제공하는 ID 공급자입니다. Symantec 은 다양한 Norton 제품들에서 수백만 명의 사용자 신원 관리를 위한 인프라를 제공합니다.	*1. 자택 주소, 전화번호, 생년월일 및/또는 신용카드 번호와 같은 사용자의 신원을 인증하는 데 도움이 되는 개인 데이터, 사용자 연락처 정보, 사용자가 Norton 계정에 입력하거나 사용자가 고객 지원과 연결 지원을 위해 제공할 수 있는 일체의 추가 개인 데이터(예: 이름, 기기 정보 등) 2. 기기 유형, 제조업체, 모델, 운영 체제와 버전을 포함한 기기, 제품, 서비스 정보와 기기 사용자 에이전트 데이터/앱 사용자 에이전트 데이터, 기기 유형, 제조업체, 모델, 운영 체제와 버전, 런타임 성능 데이터, 설치된 애플리케이션, 관련 지리적 정보, MAC 주소, IP 주소를 포함한 기기 정보와 기기 사용자 에이전트 데이터/앱 사용자 에이전트 데이터 3. 방문한 웹사이트의 URL 과 IP 주소, 검색 키워드와 결과, 잠재적인 보안 위험에 관한 정보(웹사이트가 사용자의 허가 없이 수집하려 시도하는 개인 데이터를 포함할 수 있는 잠재적으로 사기성인 것으로 간주되는 웹사이트의 URL 과 IP 주소 포함)와 같은 인터넷 사용에 관한 사용 현황 데이터	1. 개인 데이터는 Symantec 이 다음 용도로 처리합니다. • Symantec 또는 Norton Security Login 을 이용하는 믿을 만한 제 3 자를 위해 사용자 신원을 인증하기 위한 목적, • 신원 자격 증명을 발급하고 또한/또는 사용자 이름으로의 사기성 거래를 피하기 위한 목적, • 셋업 프로세스 동안 사용자를 안내하기 위한 목적, • 지원을 포함한 서비스 제공을 위해 사용자와 소통하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 기기, 제품, 서비스 정보는 Symantec 이 다음 용도로 처리합니다. • 제품과 서비스의 성능을 활성화하고 최적화하기 위한 목적, • 라이선스 관리를 위한 목적, 그리고 • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적. 3. 사용 현황 데이터는 Symantec 이 다음 용도로 처리합니다. • 사용자들에게 사이트 안전에 관해 알리기 위한 목적, • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적, 그리고 • Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton Ultimate Help-Desk & Norton Computer Tune-Up

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Ultimate Help Desk 는 사용자가 네트워크 셋업으로부터 기기 진단과 문제 해결까지 기술 문제를 지원하는 전문가와 연락할 수 있게 해줍니다. Norton Computer Tune-Up 은 Norton Ultimate Help Desk 내의 기능으로, 진단을 사용하여 사용자 기기가 새로운 기기처럼 작동할 수 있도록 도와줍니다.	*1. 귀하가 전화를 통해 Symantec 서비스 직원에게 제공하거나 Norton 서비스를 요청할 때 Symantec 온라인 인터페이스에 입력하는 요청 정보 2. 다음을 포함한 시스템 정보: 기기에서 사용한 운영 체제와 브라우저 유형과 버전, 방화벽이 활성화되어 있는지 여부, 안티바이러스 소프트웨어가 설치, 구동, 최신 상태인지 여부, 메모리와 디스크 공간, 프록시 구성, 지원 소프트웨어 도구의 디렉터리 목록, 보안과 임시 파일 설정을 포함한 브라우저 정보, 기기의 활성 포트, 호스트 파일, 네트워크 인터페이스 설정, 설치된 프로그램과 활성 프로세스 정보, 애플리케이션과 운영 체제 로그 파일 정보, 레지스트리 데이터 3. 다음을 포함한 진단 정보: 스캔한 파일 수, 발견한 위협 수, 지원 소프트웨어 도구로 교정한 위협 수, 발견한 위협 유형, 지원 소프트웨어 도구로 확인한 기기의 보안 상태(양호/보통/불량), 지원 소프트웨어 도구로 교정하지 못한 남은 위협 수와 유형	1. 요청 정보는 Symantec 이 다음 용도로 처리합니다. • 서비스 제공을 위해 사용자와 소통하기 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 시스템 정보는 Symantec 이 다음 용도로 처리합니다. • 사용자가 요청한 서비스를 제공하기 위한 목적, • 서비스 이행을 활성화하고 최적화하기 위한 목적, 그리고 • 서비스를 이용하는 동안 사용자를 안내하기 위한 목적, 3. 진단 정보는 Symantec 이 다음 용도로 처리합니다. • 이행한 서비스 결과를 사용자에게 통지하기 위한 목적, 그리고 • Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

노턴 시큐리티 VPN (전 Norton WiFi Privacy)

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
노턴 시큐리티 VPN 는 사용자 기기를 보호하고, 일체의 인터넷 연결에서 사용자 정보를 암호화하고 사용자의 개인정보 보호를 보존함으로써 사용자 데이터를 보호합니다.	1. 구독자 정보와 모바일 기기 데이터(기기 이름, 유형, OS 버전, 언어 포함) 2. 총 대역폭 사용 3. 서비스 문제의 디버그를 지원하는 임시 사용 현황 데이터	1. 구독자 정보와 모바일 기기 데이터는 Symantec 이 다음 용도로 처리합니다. • 서비스 이행을 활성화하고 최적화하기 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, • 소프트웨어 설치와 서비스를 이용하는 동안 사용자를 안내하기 위한 목적, • 서비스 제공을 위해 사용자와 소통하기 위한 목적, • 사용자가 전송하는 정보를 보호할 것임을 상기시켜 주기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 대역폭 사용 현황 데이터는 Symantec 이 청구, 네트워크 운영, 지원을 위해 처리합니다. 3. 임시 사용 현황 데이터는 Symantec 이 다음 용도로 처리합니다. • 연결하기에 가장 적절한 서버를 선택하기 위한 목적, 그리고 • Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적. 노턴 시큐리티 VPN 를 사용하는 동안, 당사는 사용자의 인터넷 트래픽을 “로그가 없는” 네트워크인 Symantec 네트워크를 통해 전송합니다. 이는노턴 시큐리티 VPN 에 연결할 때 Symantec 이 사용자의 원래 IP 주소를 저장하지 않기에, Symantec 이 개인을 식별할 수 없음을 의미합니다. 정보에 관한 로그를 보관하지 않을지라도, Symantec 의 자동 규칙 기반 트래픽 관리는 대상 웹사이트 또는 IP 주소, 원래 IP 주소를 포함한 인터넷 데이터 트래픽의 실시간 분석을 필요로 할 수 있습니다. Symantec 은 사용자가 다운로드, 사용 또는 방문하는 애플리케이션, 서비스 또는 웹사이트에 관한 정보를 저장하지 않습니다. Symantec 이 글로벌 네트워크를 관리하기에, 사용자의 인터넷 트래픽은 Symantec – Norton 글로벌 개인정보 보호정책에 설명된 바와 같이 하나 이상의 다른 국가들을 통해 전송될 수 있습니다. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton 보안 제품(Security, Internet Security, One, Antivirus & 360)

이 섹션에서는 Norton Security(표준, 디럭스, 프리미엄), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE, Norton 360MD 를 다룹니다.

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton 보안 제품은 랜섬웨어, 바이러스, 스파이웨어, 멀웨어, 기타 온라인 위협으로부터 방어해 주는 끝점 보안을 제공합니다.	1. 사용자가 Norton 계정을 만들기 위해 입력할 수 있는 *개인 데이터(예: 사용자 이름, 선택적인 사진)를 포함한 구독자 정보와 기기 데이터, 기기에 이름을 지정할 때 사용자가 포함시키는 일체의 *개인 데이터, 제공된 경우 기기를 배정받는 개인의 이름 또는 별명, 기기 사용자 에이전트 데이터/앱 사용자 에이전트 데이터(기기 유형, 제조업체, 모델, 운영 체제와 버전, 애플리케이션과 버전, 관련 지리적 정보, MAC 주소, 기계 ID, IP 주소 포함), 파일 또는 폴더 이름에 포함되어 있는 경우, 우발적으로 개인 데이터를 포함할 수 있는 설치와 운영에 관한 상태 정보, 고객 지원과 연결 지원을 위해 사용자가 Symantec 에 제공하는 일체의 추가 개인 데이터(예: 사용자 ID, 이름, 역할, 정책, 기기 정보) 2. 방문한 웹사이트의 URL 과 IP 주소, 검색 키워드와 결과, 잠재적인 보안 위험에 관한 정보(웹사이트가 사용자의 허가 없이 수집하려 시도하는 개인 데이터를 포함할 수 있는 잠재적으로 사기성인 것으로 간주되는 웹사이트의 URL 과 IP 주소 포함)와 같은 인터넷 사용에 관한 데이터 3. 다음을 포함한 기기 사용과 진단에 관한 데이터: 마지막 기기 사용 시간, 각 연결된 기기의 인터넷 사용 시간, 네트워크 연결 활동을 상세히 설명하는 게이트웨이 로그에 관한 데이터, 사용자의 허가 없이 멀웨어가 수집한 개인 데이터를 포함할 수 있는 잠재적 멀웨어로 확인된 실행 파일, 스팸으로 보고된 또는 스팸으로 잘못 식별된 사용자의 허가 아래 Symantec 에 전송한 이메일 메시지, “크래시 덤프” 정보 또는 제품과 서비스에 문제가 발생할 때 사용자가 Symantec 에 전송하기로 선택할 수 있는 보고서에 포함된 정보(이는 시스템 언어, 국가 로캘, 운영 체제, 오류 시 실행 중인 프로세스/파일을 포함할 수 있음) 4. 차단된 웹사이트, 방문한 웹사이트, 시간과 콘텐츠 필터 정보, 위험한 것으로 결정 또는 간주된 웹사이트의 URL 을 포함한 사용자가 정의하고 구성한 보호자 통제 정보와 설정	1. 구독자 정보와 기기 데이터는 Symantec 이 다음 용도로 처리합니다. • 제품과 서비스의 성능을 활성화하고 최적화하기 위한 목적, • Symantec 을 위해 사용자의 신원을 인증하기 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 서비스 제공을 위해 사용자와 소통하기 위한 목적, • 라이선스 관리를 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 인터넷 사용 현황 데이터는 다음을 위해 처리합니다. • 사용자에게 사이트 안전에 관해 알리기 위한 목적, 그리고 • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적. 3. 기기 사용 현황과 진단 데이터는 Symantec 이 다음 용도로 처리합니다. • 제품 사용을 이해하기 위한 목적, • 제품과 서비스의 보호 기능을 제공하기 위한 목적, 그리고 • Symantec 제품과 서비스를 개선하고 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적. 4. 보호자 통제 정보와 설정은 사용자가 통제 프로필에 정의한 규칙과 정책을 집행하고, 사용자가 이러한 프로필과 관련된 개인 데이터 오용을 탐지하도록 돕고, 사용자/통제 프로필과 소통하는 데 사용됩니다. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적, • 전반적인 사용자 경험을 최적화하기 위해 제품 관련 커뮤니케이션의 빈도를 이해하기 위한 목적, 그리고 • 당사의 운영 실적 개선과 관련된 다른 비사용자 특이 비즈니스와 마케팅 통찰력을 얻기 위한 목적.

Norton Safe Search, Norton Home Page, Norton Safe Web

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Safe Search 는 보다 안전한 웹 검색 경험을 제공하기 위해 검색 결과를 필터링하고 사용자에게 웹사이트 안전 등급을 제공하여 사용자를 위험한 웹사이트로부터 보호해 주는 검색 엔진 웹사이트입니다. 이는 또한 다양한 방법으로 Norton Safe Search 웹사이트에 대한 접근을 제공하는 브라우저 확장입니다. 이 확장의 다른 버전들은 사용자의 선택에 따라 a) 브라우저의 기본 검색 엔진을 Norton Safe Search 웹사이트로 재정의하거나, b) 브라우저의 기본 검색 엔진 설정을 Norton Safe Search 웹사이트로 재정의하고 브라우저의 기본 홈페이지 + 새로운 탭 설정을 Norton Home Page 로 재정의할 수 있습니다. Norton Home Page 는 Norton Safe Search 웹사이트를 활성화하는 브라우저 확장 기본 홈페이지입니다. Norton Safe Web 은 사용자가 검색 활동과 웹페이지 콘텐츠를 모니터링하기 위해 사용하기로 선택하는 브라우저 확장입니다. 이는 악의적인 웹사이트 콘텐츠,	1. 다음을 포함한 구독자 정보, 기기와 소프트웨어 데이터: 웹 브라우저 이름, 버전, 선호 언어, 운영 체제, 버전 또는 플랫폼, 사용자 기기 IP 주소 2. 다음을 포함한 서비스 사용 현황 데이터: 소셜 미디어 및 웹 메일의 링크, 웹사이트 검색 활동, 웹 검색 용어, Norton 제품들이 관리하는 다른 검색창들의 기본 입력사항, 검색 엔진 결과 3. Norton Safe Search 웹사이트와 Norton Home Page 웹사이트가 컴퓨터 또는 기기에 설치하는 쿠키, 픽셀 태그, 스크립트 또는 유사한 기술	1. 구독자 정보, 기기와 소프트웨어 데이터는 Symantec 이 다음 용도로 처리합니다. • 서비스 이행을 활성화하고 최적화하기 위한 목적, • 라이선스 관리를 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 사용자, 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하는 제품과 서비스 향성을 제공하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 서비스 사용 현황 데이터는 Symantec 이, 또한 Symantec 을 대신하여 다음 용도로 처리합니다. • 사용자에게 사이트 안전에 관해 알리기 위한 목적, • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적, 그리고 • 서비스 사용을 분석하기 위한 목적. Norton Safe Search 제품을 통해 제출되는 사용자의 검색 쿼리 요청은 귀하에게 쿼리 조사를 제공하기 위해 (미국과 캐나다의 경우) 제 3 자 검색 파트너인 Oath/Yahoo!, (미국과 캐나다 이외 국가들의 경우) IACI 로 전달할 것입니다. 또한 제 3 자 파트너들은 귀하의 Norton Safe Search 에서의 활동에 기반하여 귀하로부터 직접 정보를 수집할 수 있습니다. 당사의 제 3 자 파트너들은 검색 쿼리를 처리하기 위해 데이터 관리자와 같은 데이터를 수집할 것입니다. 이러한 데이터 수집에는 제 3 자 파트너의 개인정보 보호정책, 취급방침이 적용됩니다. Norton Safe Search 를 귀하에게 제공하기 위해, 제 3 자(즉 Symantec 회사가 아님)에게 귀하의 검색 쿼리 요청을 전달하고, 이러한 제 3 자가 요청을 처리할 것입니다. 또한 제 3 자 파트너는 귀하의 Norton Safe Search 에서의 활동을 통해 귀하로부터 직접 정보를 수집할 수 있습니다(총체적으로 "제 3 자 데이터"). 3 자 파트너는 검색 쿼리의 처리 측면에서 데이터 관리자일 것입니다. 따라서 귀하의 제 3 자 데이터를 수집, 사용, 공개, 보관 또는 달리 처리할 방법을 결정하는 것은 Symantec 이 아닌 제 3 자 파트너입니다. 귀하의 제 3 자 데이터에는 검색 쿼리를 실행하기 위한 데이터 처리에 관한 제 3 자 파트너의 개인정보 보호정책이 적용됩니다. 제 3 자 파트너의 개인정보 보호정책을 참조하십시오. 3. 쿠키와 유사한 트래커는 다음의 기능 사용 선호도와 기록을 위해 처리합니다. 쿠키에 관한 추가 정보는 상기 Symantec – Norton 글로벌 개인정보 보호정책의 "추적 기술, 쿠키, 추적 금지" 섹션을 참조하십시오. 익명화 IP 주소와 제품 사용 정보는 Google Analytics 의 측정 프로토콜이 중요한 오류 통계 분석과 관리를 위해 처리합니다. Google Analytics 데이터 보호 조치에 관한 정보를 보려면 여기를 클릭하십시오. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, 그리고 • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적.

피싱, 다른 위협으로부터 사용자를 보호하기 위해 평판 서비스와 웹페이지 콘텐츠 분석을 사용합니다.		

Norton Security Toolbar

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Security Toolbar 에는 a) Microsoft Internet Explorer 에 대한 추가 기능, b) Google Chrome 의 브라우저 확장이란 두 가지 변형이 있습니다. 두 변형은 사용자가 자신의 검색 활동과 웹 페이지 콘텐츠를 모니터링하는 데 사용합니다. 이는 악의적인 웹 콘텐츠, 피싱, 다른 위협으로부터 사용자를 보호하기 위해 평판 서비스와 웹페이지 콘텐츠 분석을 사용합니다. Internet Explorer 변형은 브라우저 사용자 인터페이스 내에서 Norton Identity Safe 자격 증명 모음 정보에 접근하고 이를 사용할 수 있게 해줍니다. 이는 또한 Norton Safe Search 웹사이트에서 검색을 실행할 검색창을 제공합니다. Google Chrome 변형은 Norton Safe Search 웹사이트에서 검색을 실행할 검색창을 제공합니다.	1. 다음을 포함한 기기와 소프트웨어 데이터: 웹 브라우저 이름, 버전, 선호 언어, 운영 체제, 버전 또는 플랫폼, 사용자 기기 IP 주소 2. 다음을 포함한 제품 사용 데이터: 웹사이트 검색 활동, 제한된 웹사이트 검색 기록, 웹 검색 용어, Norton 제품들이 관리하는 다른 검색창들의 기본 입력사항, 검색 엔진 결과 3. Norton Safe Search 웹사이트와 Norton Home Page 웹사이트가 컴퓨터 또는 기기에 설치하는 쿠키, 픽셀 태그, 스크립트 또는 유사한 기술	1. 기기와 소프트웨어 데이터는 Symantec 이 다음 용도로 처리합니다. • 서비스 이행을 활성화하고 최적화하기 위한 목적, • 라이선스 관리를 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 사용자, 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하는 제품과 서비스 향성을 제공하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 제품 사용 현황 데이터는 Symantec 이, 또한 Symantec 을 대신하여 다음 용도로 처리합니다. • 사용자에게 사이트 안전에 관해 알리기 위한 목적, • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적, 그리고 • 서비스 사용을 분석하기 위한 목적. 3. 쿠키와 유사한 트래커는 다음의 기능 사용 선호도와 기록을 위해 처리합니다. 쿠키에 관한 추가 정보는 상기 Symantec – Norton 글로벌 개인정보 보호정책의 “추적 기술, 쿠키, 추적 금지” 섹션을 참조하십시오. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, 그리고 • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적.

Norton Identity Safe

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Identity Safe 에는 a) Norton Security 구성요소, b) Internet Explorer 를 제외한 모든 주요 브라우저의 브라우저 확장의 두 가지 변형이 있습니다. 모든 변형은 사용자 이름, 암호, 온라인 활동 실행에 유용한 다른 정보를 관리하는 암호 관리자입니다.	1. 다음을 포함한 구독자 정보, 기기와 소프트웨어 데이터: 웹 브라우저 이름, 버전, 선호 언어, 운영 체제, 버전 또는 플랫폼, 사용자 기기 IP 주소, 사용자 이름, 암호, 웹사이트 주소, 물리적 주소, 결제 계좌 번호, 만료 정보, 자유 형식 텍스트를 포함할 수 있는 사용자가 공개하는 기타 개인 데이터 2. 다음을 포함한 서비스 사용 현황 데이터: 웹사이트 검색 활동, 웹 검색 용어, Norton 제품들이 관리하는 다른 검색창들의 기본 입력사항, 검색 엔진 결과	1. 기기와 소프트웨어 데이터는 Symantec 이 다음 용도로 처리합니다. • 서비스 이행을 활성화하고 최적화하기 위한 목적, • 라이선스 관리를 위한 목적, • 사용자 경험을 개인화하고 개선하기 위해 제품 사용과 기본 설정을 이해하기 위한 목적, • 소프트웨어 설치 프로세스 동안 사용자를 안내하기 위한 목적, • 사용자, 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하는 제품과 서비스 향성을 제공하기 위한 목적, 그리고 • 자사 및 제 3 자 콜 센터를 통해 제공하는 서비스의 고객 만족도를 개선하기 위한 목적. 2. 제품 사용 현황 데이터는 Symantec 이, 또한 Symantec 을 대신하여 다음 용도로 처리합니다. • 사용자에게 사이트 안전에 관해 알리기 위한 목적, • 안전하지 않은 웹사이트로의 검색을 차단하기 위한 목적, 그리고 • 서비스 사용을 분석하기 위한 목적. 익명화 IP 주소와 제품 사용 정보는 Google Analytics 의 측정 프로토콜이 중요한 오류 통계 분석과 관리를 위해 처리합니다. Google Analytics 데이터 보호 조치에 관한 정보를 보려면 여기를 클릭하십시오. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적, 그리고 • 가용성과 대응 시간 측면에서 제품 성능을 모니터링하고 개선하기 위한 목적.

Norton Family Premier

제품/서비스 설명	데이터 접근 및 수집	데이터 처리
Norton Family Premier 는 구독자가 보호하기로 선택하는 보호 대상 사용자와 기기를 보호하도록 도와주고, 보호자 통제는 구독자 정의, 구독자 관리 보호 설정과 기능을 통해 적용됩니다. Norton Family Premier 에 관한 추가 상세정보는 다음의 "Norton Family Premier 추가 정보" 섹션을 참조하십시오.	*1. 다음과 같은 구독자 정보: 구독자 이름, 이메일 주소, 구독자의 계정을 보호하는 암호를 포함하되 이에 국한되지 않는 관리자 연락처 정보, 서비스 구성 또는 일체의 다른 후속 서비스 통화 동안 구독자가 제공하는 개인 데이터, 2. 다음을 포함한 기기와 소프트웨어 데이터: 구독자 또는 보호 대상 사용자 기기에 Norton Family 클라이언트 소프트웨어 설치 상태, 소프트웨어 구성, 제품 상세정보, 설치 상태, 라이선스 상태, 라이선스 권리 정보, 라이선스 ID, 라이선스 사용, 기기 이름, 유형, OS 버전, 언어, 위치(글로벌 위치 시스템, GPS), 브라우저 유형과 버전, 기기 하드웨어, 소프트웨어, 애플리케이션 인벤토리, 애플리케이션과 데이터베이스 접근 구성, 정책 요건과 정책 준수 상태, 애플리케이션 예외와 워크플로 오류 로그, *3. 다음을 포함한 구독자가 Symantec 에 공개하기로 선택하는 보호 대상 사용자 정보: 이름, 성별, 연령, 출생 연도, 아바타 이미지, 보호 대상 사용자와 관련된 공식 ID 번호의 마지막 6 자리 수(예: 이용 가능한 경우: 사회보장번호, 국가 ID 번호), 이메일 주소, 휴대폰 번호, 학교 이름 또는 구독자가 보호하고 싶어하는 일체의 다른 정보, 기계 로그인 계정 상세정보, 국가, 시간대, 4. 구독자의 독립적 선택에 의거한 경우를 포함한 구독자가 Symantec 에 모니터링하도록 지시하는 보호 대상 사용자 네트워킹 활동 정보: 온라인과 모바일 기기 활동과 위치, 보호 대상 사용자가 방문하려 시도하는 웹사이트와 제품이 보호 대상 사용자의 방문을 차단하는 웹사이트, 보호 대상 사용자가 사용하는 온라인 검색 용어, 구독자가 애플리케이션 모니터링을 활성화한 경우, 보호 대상 사용자가 기기에 설치 또는 제거하는 애플리케이션, 보호 대상 사용자의 기기 사용 시간, *보호 대상 사용자의 프로필 이름, 프로필 URL, 연령, Facebook 프로필 ID, 방문한 비디오, 구독자가 비디오 모니터링을 활성화한 경우, 보호 대상 사용자가 YouTube.com 및/또는 Hulu 에서 시청하는 비디오.	1. 구독자 정보는 Symantec 이 다음 용도로 처리합니다. • Norton Family 성능을 활성화하고 최적화하기 위한 목적, • 지원 또는 디버깅 지원을 제공하기 위한 목적, • 구독자의 허가에 따라 또는 해당 법률에서 달리 허용하는 대로 구독자에게 판촉 정보를 전송하기 위한 목적, 그리고 • 구독자의 Norton 계정을 셋업하기 위한 목적. 2. 기기와 소프트웨어 데이터는 Symantec 이 다음 용도로 처리합니다. • 제품의 적절한 기능을 보장하고 구독자가 요청한 서비스를 제공하기 위한 목적, • 라이선스 관리를 위한 목적, • 제품의 설치 성공률을 평가하고 개선하기 위한 목적, • Symantec 제품과 서비스를 개선하고 구독자와 보호 대상 사용자의 네트워크, 기기, 데이터, 신원을 보다 효과적으로 보호하기 위한 연구 개발을 위한 목적, 3. 보호 대상 사용자 정보는 다음을 위해 처리합니다. • 구독자와 보호 대상 사용자를 Symantec 에 식별하고 인증하기 위한 목적, • 구독자가 보호 대상 사용자의 개인 데이터 오용을 탐지하도록 돕기 위한 목적, 그리고 • 서비스 제공을 위해 구독자, 구독자의 허가 시 보호 대상 사용자와 소통하기 위한 목적. 4. 보호 대상 사용자 활동 정보는 다음을 위해 처리합니다. • 구독자가 보호 대상 사용자 기기의 온라인 활동을 감독하도록 돕기 위한 목적, • 설치된 멀웨어로 인한 손상을 제한하기 위한 목적, • 보호 대상 사용자 기기의 온라인 활동에 관한 구독자 정의 규칙의 집행을 돕기 위한 목적, • 보호 대상 사용자가 온라인 또는 SMS/MMS 커뮤니케이션을 통해 위협에 노출되는지 구독자가 탐지할 수 있게 하기 위한 목적, 그리고 • 구독자가 이러한 위협으로부터 보호 대상 사용자를 보호하도록 돕기 위한 목적. 또한 Symantec 은 다음을 위해 수집한 데이터로부터 도출한 통합, 비식별화, 익명화 또는 달리 신원 확인 불가 데이터(예: 통계)를 사용할 것입니다. • 전반적인 사이버 보안 연구를 수행하기 위한 목적, • 파일 샘플 분석을 통한 멀웨어와 사이버 위협 탐지를 개선하기 위한 목적, • 보안, 신원 절도 위험/동향을 추적하고 보고서를 발표하기 위한 목적, 그리고 • 통합 사용자 기반에서 동향 분석과 비교를 포함한 제품 배포의 통계 분석을 수행하기 위한 목적.

Norton Family Premier 추가 정보

구독자가 서비스를 활성화하기로 선택하는 경우, Norton Family는 보호 대상 사용자가 자신의 개인 데이터를 공개하는 것을 허용하지 않을 것입니다.

구독자가 소재한 국가 또는 지역의 해당 법률에서 허용하는 경우, Symantec 은 구독자가 보호 대상 사용자의 휴대폰으로/으로부터 전송되는 텍스트("SMS")와 멀티미디어("MMS") 메시지를 차단 또는 모니터링할 수 있게 해주는 **텍스트 메시지 감시 서비스**, **위치 모니터링 서비스**를 제공할 수 있습니다. SMS 와 MMS 교환 및/또는 위치 모니터링과 이러한 모니터링에 관한 기록 사용은 구독자에게 적용되는 현지 법률에 의해 제한되거나 금지될 수 있습니다. 구독자는 이 기능을 활성화하기 전 현지 당국에 반드시 문의해야 합니다.

구독자가 위치 모니터링 서비스를 활성화하는 경우, Norton Family 는 GPS 를 사용하여 구독자가 지정한 모바일 기기의 지리적 위치를 추적하고 수집하라는 구독자의 지시를 이행할 것입니다. Norton Family 가 지정된 기기의 지리적 위치를 추적, 수집, 사용 또는 공개하기 위해서는 구독자의 동의, 경우에 따라 모바일 기기 사용자의 동의 또는 이러한 사용자의 부모 책임을 이행하는 후견인의 동의가 필요합니다. 관련 동의는 Norton 온라인 포털을 통해, 및/또는 경우에 따라 제품에서 받고, 구독자가 Symantec 온라인에서 이 서비스를 구매하기 위해 결제 카드 정보를 입력할 때 확인받습니다. 귀하는 언제든지 동의를 취소할 수 있습니다. 취소 방법에 관한 자세한 정보는 Symantec – Norton 글로벌 개인정보 보호정책의 "**귀하의 개인정보 보호 권리**" 섹션을 참조하십시오. 서비스 종료 후, 이 서비스와 관련된 구독자의 계정 정보는 삭제될 것입니다.

구독자가 지정된 모바일 기기에 애플리케이션을 다운로드한 후, Symantec은 애플리케이션이 사용되고 있지 않은 경우에도 기기의 지리적 위치를 수집할 수 있습니다. 당사는 구독자가 기기를 찾을 수 있도록 이러한 지리적 위치 정보를 구독자에게만 공개하고, 구독자가 요청한 서비스와 기능을 제공하기 위한 운영상의 용도로만 이를 처리할 것입니다. 구독자는 부모로서의 책임이 없는 일체의 개인과 관련된 데이터, 위치, 활동 또는 일체의 다른 측면을 모니터링하는 데 제품의 위치 감시 서비스를 사용할 수 없습니다. 유럽 경제 지역의 구독자들은 부모로서의 책임이 있는 보호 대상 사용자들(특히 이들이 13세 이상인 경우)과 이에 관해 이야기하고, 문제의 보호 대상 사용자가 구독자의 제품 및 관련 서비스 사용이 무엇을 의미하는지 이해할 수 있도록 필요한 모든 조치를 취해야 합니다. 제품 및 관련 서비스를 사용하기로 선택하는 경우, 구독자와 보호 대상 사용자의 관계, 보호 대상 사용자에 대한 부모로서의 책임에 적용되는 모든 법률과 규제를 준수하는 것은 전적으로 구독자의 책임입니다.

텍스트 메시지 감시

기본 값으로, 텍스트 메시지 감시는 꺼져 있습니다. 구독자는 별도로 텍스트 메시지 감시 기능을 켜고 이러한 감시를 이행할 모바일 기기에 Norton Family를 설치해야 합니다. 활성화되는 경우, 텍스트 메시지 감시는 지정된 기기로부터 다음 정보를 수집합니다.

- 모니터링하는 기기의 휴대폰 번호, 해당 기기가 SMS와 MMS 커뮤니케이션을 교환하는 상대방 기기의 휴대폰 번호,
- 지정된 기기가 수신 또는 전송하는 SMS 메시지의 콘텐츠(MMS 교환의 경우, Symantec은 교환하는 일체의 멀티 미디어 콘텐츠를 기록 또는 수집하지 않을 것이며, MMS 교환이 이루어졌다는 사실만을 수집할 것임),
- 이용 가능한 경우, 지정 기기에 SMS와 MMS 커뮤니케이션을 전송하거나 이로부터 커뮤니케이션을 수신하는 모바일 번호와 관련된 지정된 기기의 주소록 이름,
- 대화 날짜/시간 스탬프,
- 지정된 기기의 위치,
- 지정된 기기의 주소록에 포함되어 있는 경우, 당사자 전화번호, 관련 이름을 포함한 차단된 SMS/MMS 메시지의 이벤트 로그.

구독자가 지정한 모바일 기기가 전송 및/또는 수신하는 SMS 또는 MMS 메시지 모니터링을 시작하기 전, Symantec은 지정된 기기에 SMS 알림을 전송하여 제품이 지정된 기기에서 교환하는 SMS 또는 MMS 메시지 콘텐츠를 기록하고 모니터링하라는 구독자의 지시를 이행할 것임을 기기 사용자에게 경고할 것입니다. 이 SMS 경고를 수신한 후, 지정된 기기에서 SMS 또는 MMS 메시지 교환이 계속되는 경우, 본 취급방침에 기술된 용도의 메시지 기록과 모니터링이 구독자의 지시에 따라 시작될 것입니다. Symantec은 1달에 한 번 또는 새로운 대화가 있을 때마다 지정된 기기에 동일한 SMS 경고를 재전송할 것입니다.

구독자가 특정 상대방과의 모든 SMS 또는 MMS 메시지(들)을 차단하기로 선택하는 경우, 당사는 지정된 기기의 사용자에게 이를 경고하고, 상대방에게 메시지가 차단되고 메시지가 전달될 수 없음을 알리는 텍스트 메시지를 전송합니다.