



PISFAIR 2025

데이터는 멈추지 않는다

트렐릭스코리아 허효승 이사





사용자의 실수로 인한 유출



내부 사용자의 의한 유출



해킹 사고에 의한 유출

그럼 어떻게... ?



정말로 중요한 데이터는 누가 가지고 있나?

Breaches

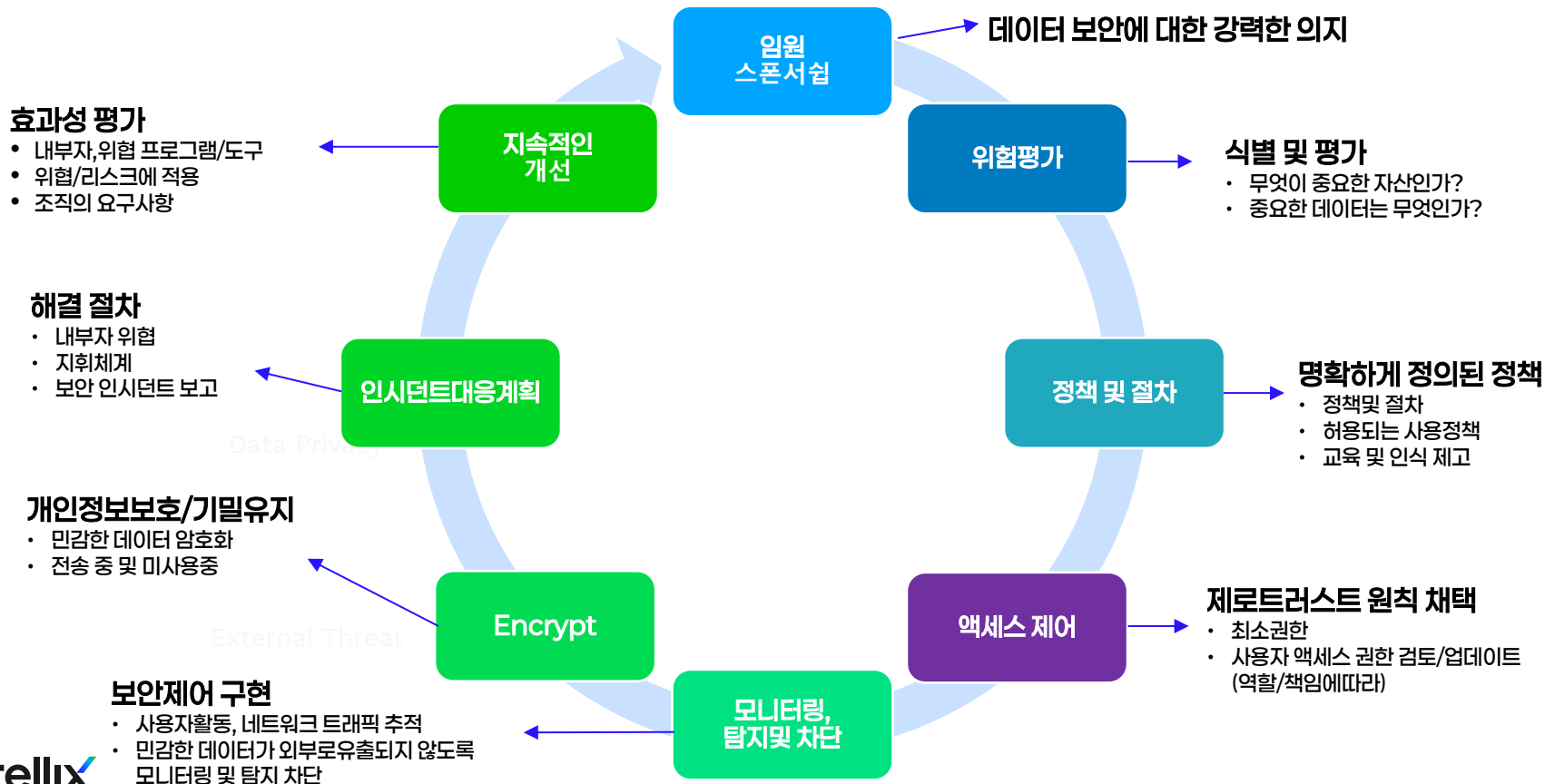


“데이터 유출 사건의 **약 75%**
사람의 실수나 악의적인 내부자에 의해 발생”

2024년 Verizon 데이터 유출 조사 보고서



내부자 위협 데이터 보안의 핵심 요소



데이터의 위치와 보호 방법을 결정하는 것은 단순화해야 할 과제



Data on the Endpoints



Data in Email



Data in the Network













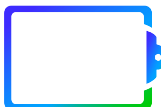

Data in the Cloud

데이터 정책 및 규칙 기능	
로그	로그 전용 정책에 플래그를 지정하는 이벤트 기록
모니터링	데이터보안 팀에 알림이 전송되고 이벤트를 분류
확인	직원이 응답이 필요한 팝업 알림
차단	정보 전송이 차단되고 최종 사용자 커뮤니케이션을 수신

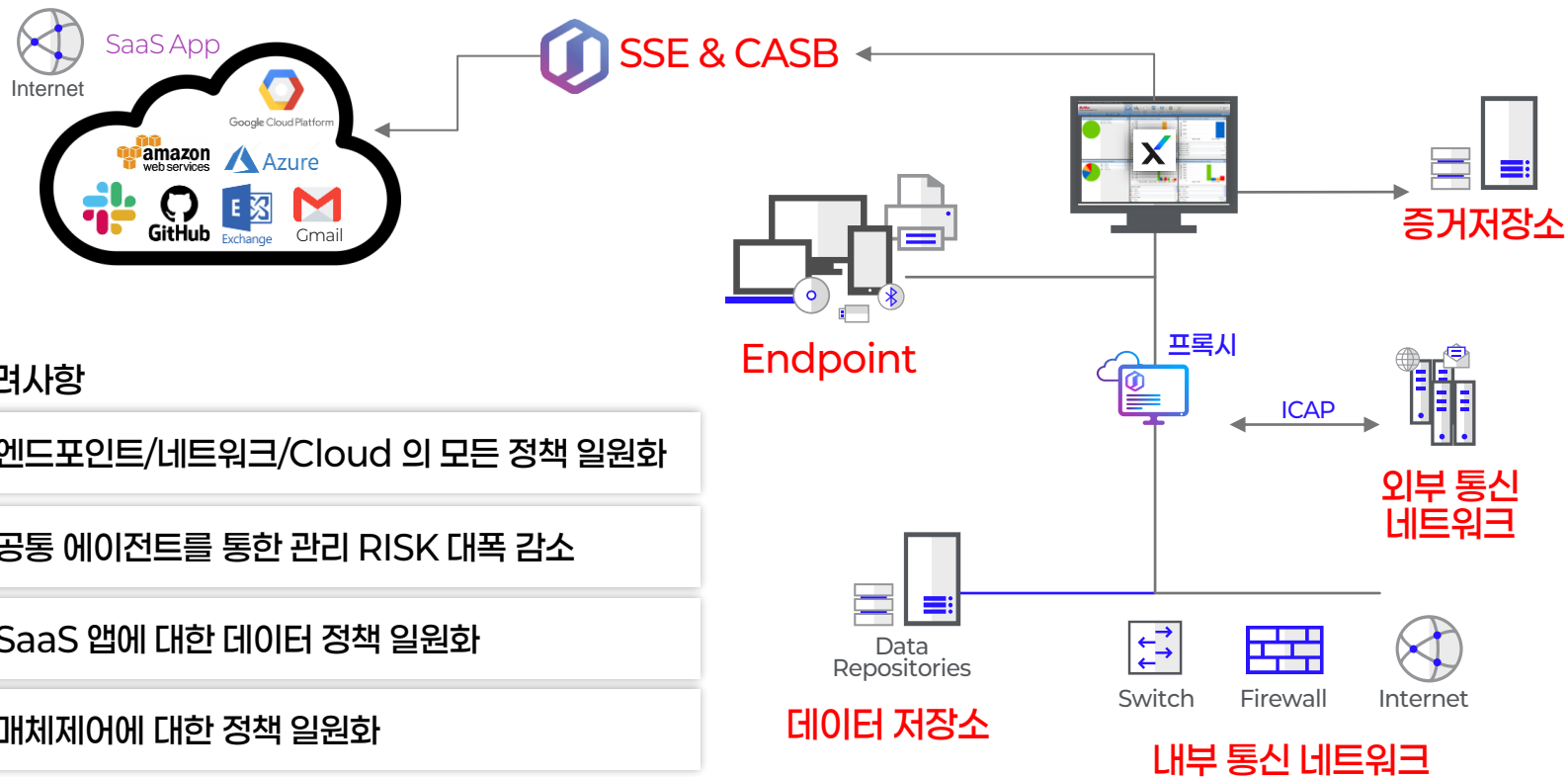
구분	고객에 대한 위험
컴플라이언스 / 규제 중요 데이터에 대해 탐지하는 정책. 예: PII, PCI, PHI, 중요 데이터	보고 및/또는 벌금이 부과되는 규정 준수 관련 데이터.
비즈니스 데이터 비즈니스 단위가 소유한 특정 중요 데이터를 탐지하는 정책. 예: 재무 결과, M&A, 법무	민감한 데이터의 오용/유실은 평판과 비즈니스 파트너십에 부정적인 영향
IT 보안 조사 제한된 시간 및 제한된 범위에서 조사	평판에 부정적인 영향.

주요 데이터 유출 경로

Trellix Data Security로 주요 데이터 유출 경로에 대한 통합 방어

Data Types	Data Loss Vectors				How to
Data-in-motion 이동중인 데이터					네트워크 모니터링 클라우드 모니터링
	Email/IM	Web Post	Network Traffic	Cloud Service	
Data-at-Rest 저장된 데이터					내부 네트워크 암호화
	File Share	Database	Endpoint	Cloud Storage	
Data-in-Use 사용중인 데이터					엔드포인트 매체제어 파일암호화 클라우드 모니터링
	Removable Media	Email/IM	File & Clipboard	Cloud Service	

데이터의 모든 경로 보안을 위한 구성 아키텍처

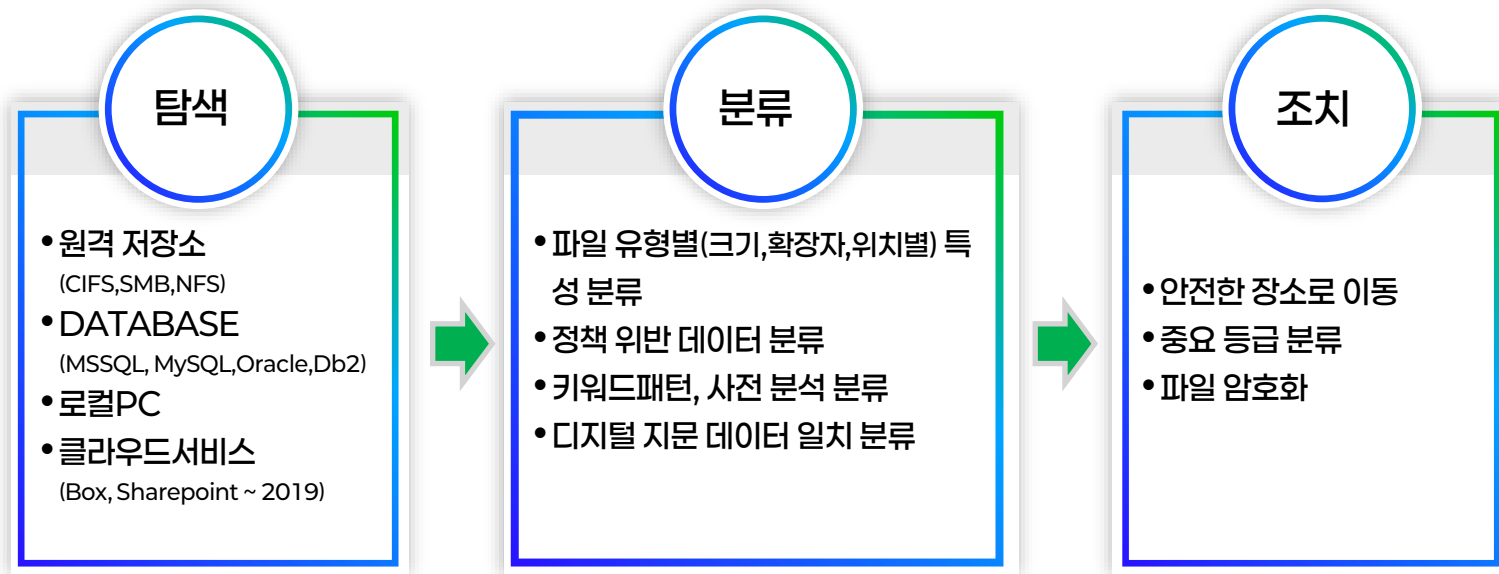


고려사항

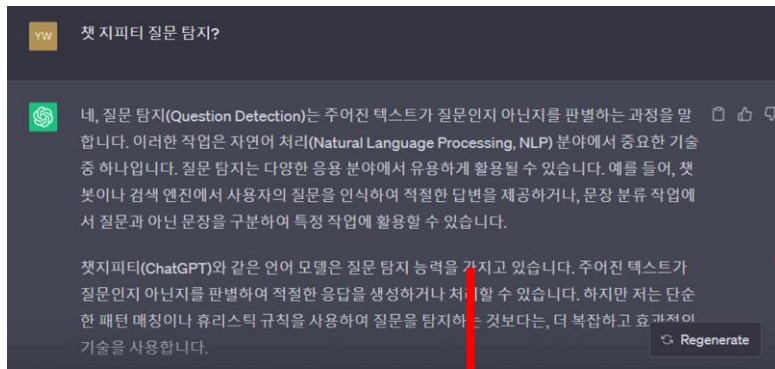
- 엔드포인트/네트워크/Cloud 의 모든 정책 일원화
- 공통 에이전트를 통한 관리 RISK 대폭 감소
- SaaS 앱에 대한 데이터 정책 일원화
- 매체제어에 대한 정책 일원화

중요 정보 탐색을 통한 식별

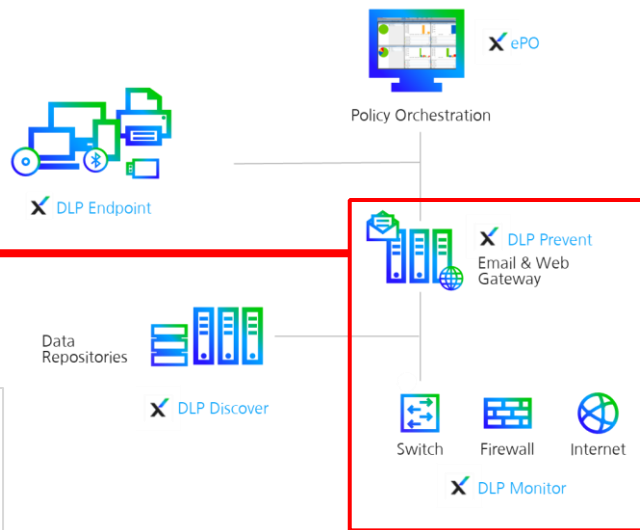
사전 정의된 분류 기준을 통해 내부의 저장소, 데이터베이스, PC 등을 검색 하여 대응할 수 있는 기능 제공



생성형 AI의 웹 콘텐츠 모니터링 및 차단

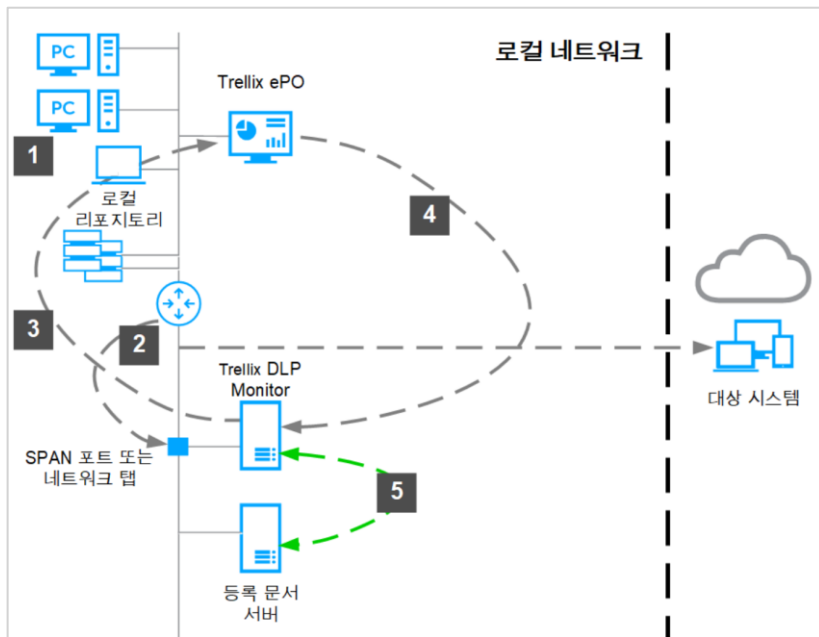


종류	총 일치 개수
<input checked="" type="checkbox"/> Capture keyword search '캡처'	4
일치	
...3da674&pid=Wdp", "title": "경기 의정부시에서 흥기를 들고 뛰어다닌다는 오인 신고로 중학생 A군이 경찰에 검거되는 과정에서 다치는 사고가 발생했다. 온라인 커뮤니티 캡처", "caption": "경기 의정부시에서 흥기를 들고 뛰어다닌다는 오인 신고로 중학생 A군이 경찰에 검거되는 과정에서 다치는 사고가 발생했다. 온라인 커뮤니티 캡처", "source": "...	
... 온라인커뮤니티 캡처", "caption": "경기 의정부시에서 흥기를 들고 뛰어다닌다는 오인 신고로 중학생 A군이 경찰에 검거되는 과정에서 다치는 사고가 발생했다. 온라인커뮤니티 캡처", "source": "msn", "colorSamples": [{"tsDarkMode": true, "hexColor": "#44392C", "tsGreyScale": false}], "tsDa...	
... Wdp", "title": "인도 여행 중 현지 경찰에게 사기를 당해 화제가 됐던 벨스 유튜브 핏볼리가 여행 어플리케이션 회사에게 렌터카 비용 전액을 환불받았다.(사진=핑크볼리 유튜브 캡처) *재판매 및 DB 금지", "caption": "인도 여행 중 현지 경찰에게 사기를 당해 화제가 됐던 벨스 유튜브 핏볼리가 여행 어플리케이션 회사에게 렌터카 비용 전액을 환불받았다...", "source": "...	
... 지", "caption": "인도 여행 중 현지 경찰에게 사기를 당해 화제가 됐던 벨스 유튜브 핏볼리가 여행 어플리케이션 회사에게 렌터카 비용 전액을 환불받았다.(사진=핑크볼리 유튜브 캡처) *재판매 및 DB 금지", "focalRegion": {"x1": 233, "x2": 308, "y1": 186, "y2": 261}, "source": "msn", "colorSamples": [{"tsDa...	



퇴사자의 데이터 검색

네트워크 캡처 기능을 이용하여 암호화 되지 않은 트래픽을 저장하여 검색



✓ 주요 모니터링 프로토콜

SMTP, IMAP, POP3, HTTP, LDAP, Telnet, FTP, IRC, SMB, SOCKS

✓ SPAN/TAP 구성 지원

✓ 데이터 캡처를 기반으로 민감 데이터 전송을 모니터링하고 기록

✓ 내부 유입되는 정책에 대한 사전 모니터링

데이터는 본인 책임

 Trellix Data Loss Prevention

데이터 유출사유입력

사내정책상 유출 및 보관이 금지된 문서/파일이 발견되었습니다. 해당 정보의 취급 사유와 반출 사유를 작성하여 주시기 바랍니다.

분류가 일치하는 문자열이 없음

자세한 정보를 보려면 [인시던트를 트리거한 내용에 대한](#)

정당성 유형:

사유입력 ▼

설명:

(*) 정당성 설명을 추가하십시오

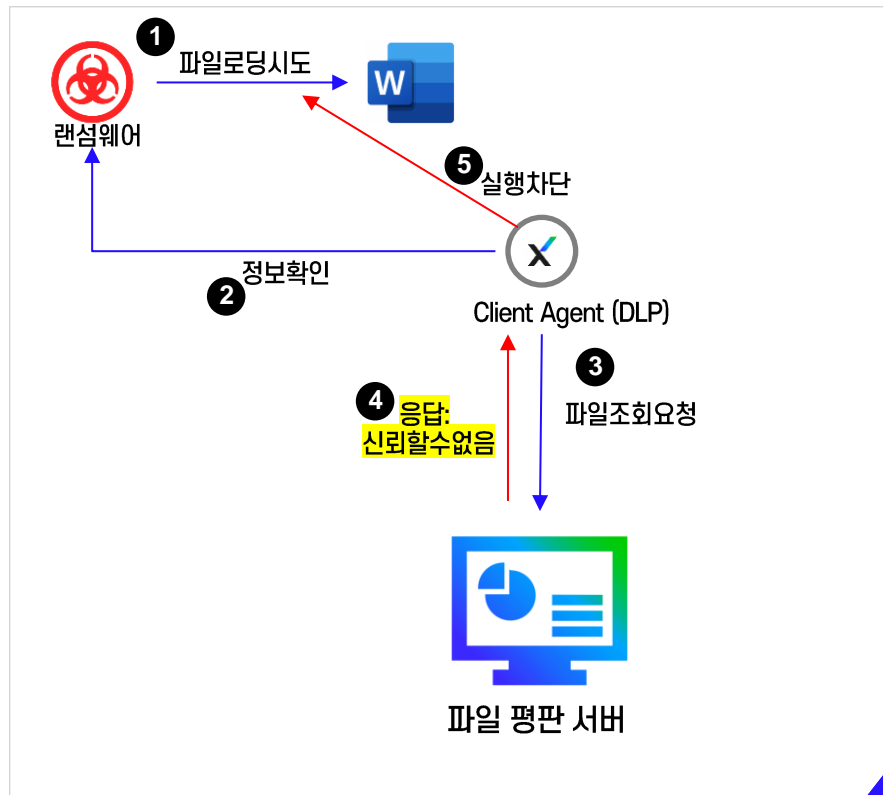
차단* 취소*

- 일부 규칙에는 사용자가 정책 위반에 대한 사유를 선택하거나 입력.
- 승인 결재를 진행하더라도 본인의 관리 데이터는 직접 관리해야 함.

안전한 소프트웨어로 실행할 수 있는 방법

평판정보, 악성코드 정보를 통합하여
관리되는 시스템 구축

- ✓ 문서 파일에 대한 등급에 따라 차등 적용
- ✓ 특정 사용자, 그룹등 에 대하여 차등 적용 (VIP, AD 연동 등)
- ✓ 신규 유입파일 및 내부 비인가 파일에 대해서 적용
- ✓ 알 수 없는 파일에 대하여 VX 또는 GTI 에 추가 쿼리



데이터 보안에 AI를 활용하려면...

AI를 활용한 데이터 분류

- 최신 머신 러닝 모델을 활용하여 다양한 유형의 민감한 데이터 **자동인식**
- AI를 활용하여 탐지를 지속적으로 조정하고, 더 높은 일치 신뢰도를 제공하고, 오탐을 낮춤

AI를 활용한 정책 생성

- 자연어 인터페이스를 통해 DLP **정책 생성 간소화** 및 개선
- 사용자의 요구사항을 AI를 통해 즉각 정책에 반영

AI 기반 이벤트 관리

- 데이터의 **우선순위**를 정하고 이벤트에 보다 효율적으로 대응하여 데이터 침해 위험을 최소화.
- AI 기반 리스크, 심각도 관리 및 조치 효율 향상
- 위협에 대한 상황 별 통찰력과 잠재적 격차를 해소하기 위한 조언 확보

데이터 보안에 AI를 활용하려면...

- DLP 발생 사례를 통합하고 심각도를 판단하여, 주의가 필요한 사례에 우선순위를 지정할 수 있도록 지원
- Trellix XDR 연계 하여 위협 URL 자동 차단 정책 변경
- 이벤트에 요약 정보 제공 및 SOC 하이라이트
- Trellix Wise 와 직접 채팅 기능 제공



The Trellix logo is centered on a solid blue background. It features a decorative border at the top and bottom consisting of a grid of small, white, slanted lines. The word "Trellix" is written in a white, sans-serif font, with the final 'x' having a distinctive slanted top bar.

Trellix