Qualys

AI가 바꾸는 사이버 리스크 관리

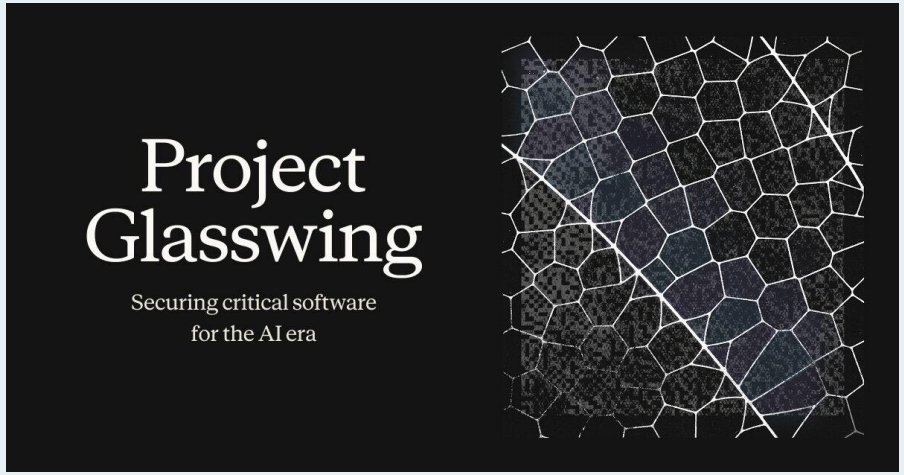
: 자동화와 보안 거버넌스의 새로운 패러다임

김주형 (Aaron Kim)
상무이사
Qualys Korea
Account Executive & Technical Account Manager

사이버 보안의 변곡점:
사이버 무기로서의 프론티어 AI의 부상

2026년 4월 7일, Anthropic은 차세대 최첨단 AI 모델인 Claude Mythos의 프리뷰를 공개했습니다.

OpenAI, Meta, DeepSeek와 같은 다른 AI 연구소들도 이에 뒤이어 각자의 최첨단(Frontier) AI 모델을 선보였습니다.



Mythos 및 기타 AI 모델의 영향

01 취약점의 기하급수적 증가

02 NVD가 대부분의 CVE에 대한 추가 분석(Enrichment)을 제공하지 못하고 있음

03 취약점 악용까지 걸리는 시간이 수개월·수주에서 수시간으로 단축됨

취약점 악용의 주된 접근 경로

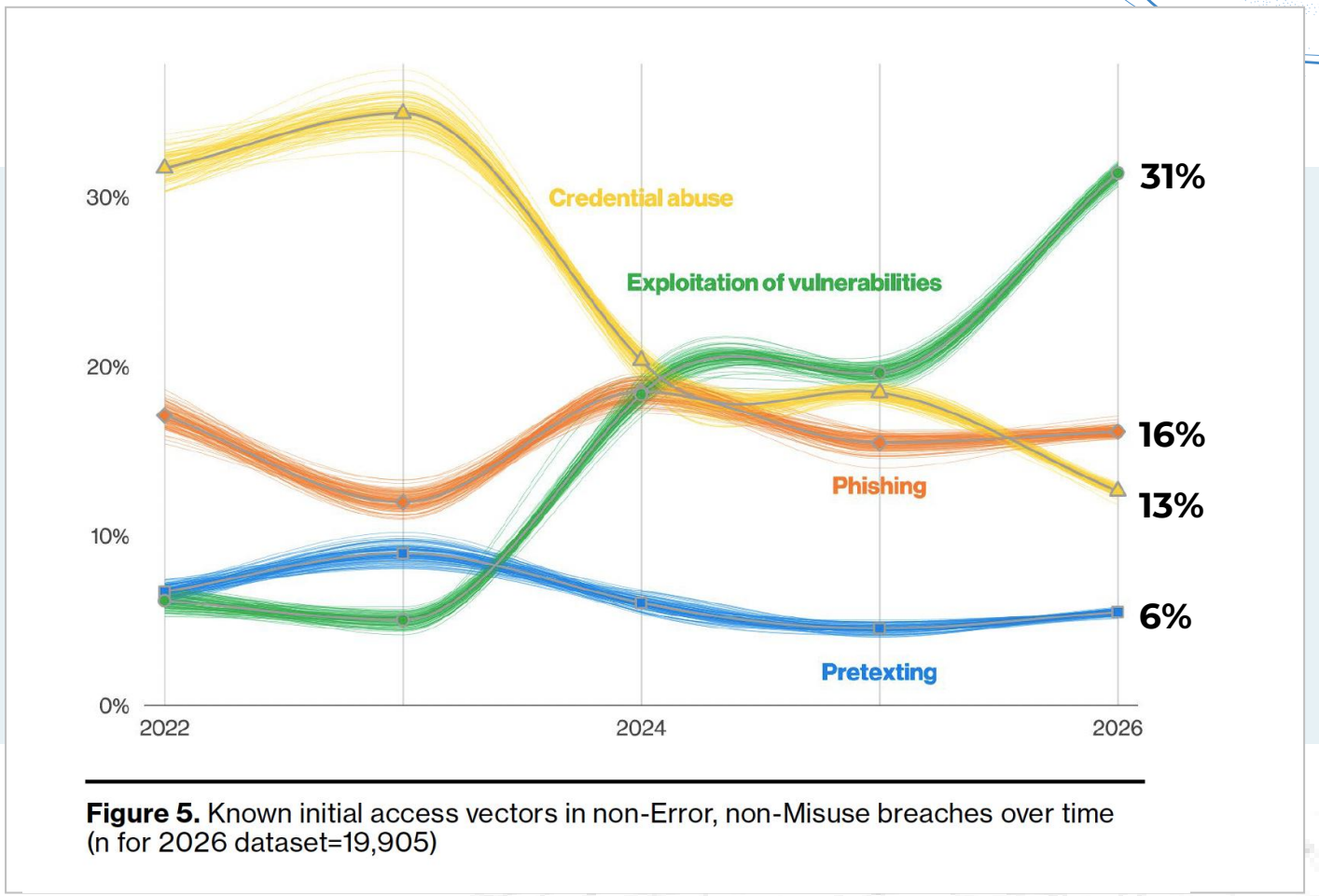


Figure 5. Known initial access vectors in non-Error, non-Misuse breaches over time (n for 2026 dataset=19,905)

경영진과 CISO들이 알고 싶어 하는 것

AI로 인해 발생하는 이러한 위험에 대해 어떻게 대응하고 있습니까?

더 신속한 대응을 위해 인력을 늘리는 것이 귀하의 답변인가요?

경영진과 CISO들이 듣고 싶어 하는 것

AI가 주도하는 자율형 공격에 맞서,
AI 기반의 자율형 대응 및 복구 체계를 구축하고 있습니다.

자율형 복구(Autonomous Remediation)를 어떻게 운영에 적용할 수 있을까요?

자율적 문제 해결을 실무에 적용하는 단계

제로데이 취약점 조치

- 패치 및 설정변경을 통한 대응방안 제공
- 운영 안정성을 보장하는 자동화 기능 제공

초(超)우선순위화

- 위협 수준, 비즈니스 영향도 및 자산 중요도를 기반으로 우선순위 결정
- 기존 보안 통제를 고려하여 실제 악용 가능성 검증

AI 수준 초고속 탐지

- 취약점 공개 즉시 탐지
- 온프레미스, 클라우드, 애플리케이션 및 컨테이너 전 영역에 대한 가시성 및 보호 제공

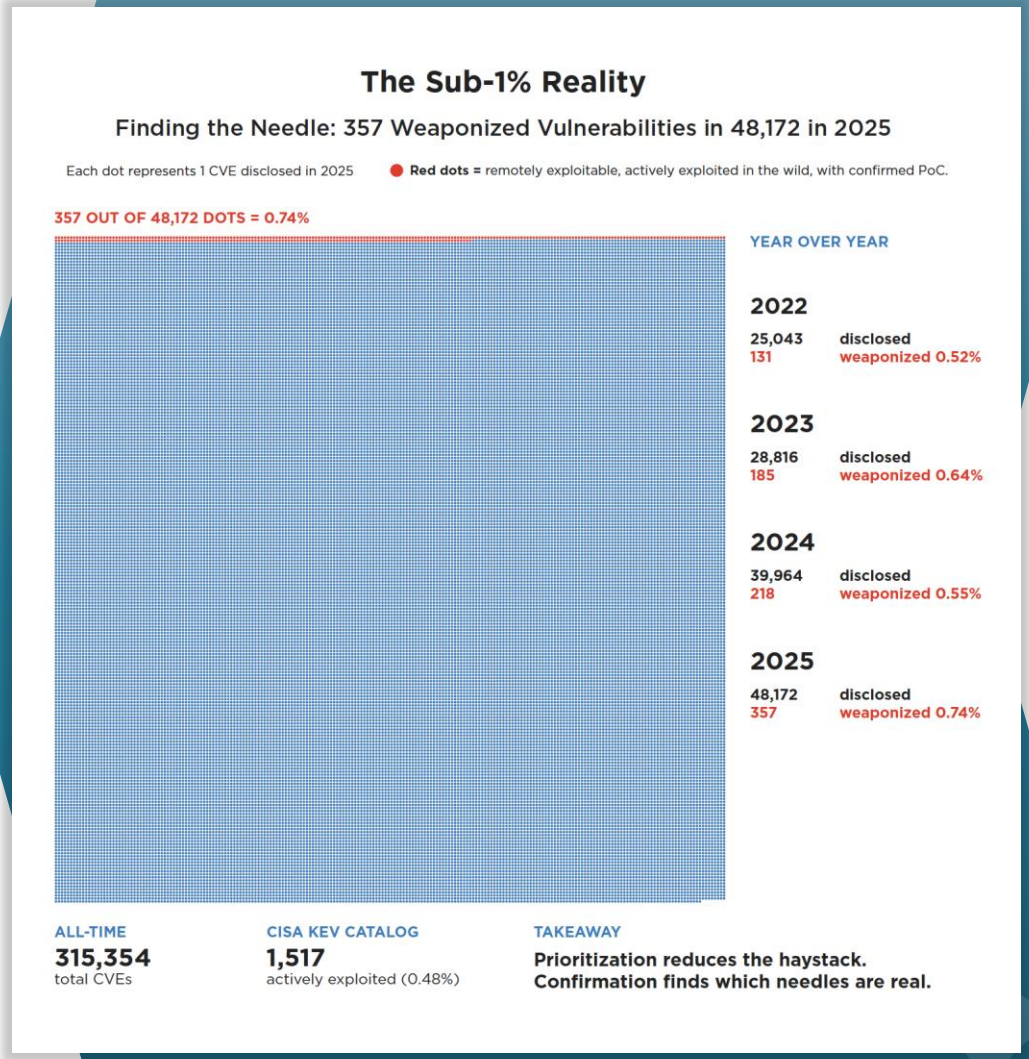
제로데이 취약점 대응의 필요성

안정적인 운영 복원력을 보장하기 위해서는 다음 요소들이 필수적입니다.

- ✓ 패치 신뢰도 점수
- ✓ 패치리스(Patchless) 복구·완화 조치
- ✓ 단계적 배포
- ✓ 롤백(복구) 기능

초(超)우선순위 설정의 필요성

- 대부분의 조직은 실제 위험이 아닌 이론적 위험을 평가하고 대응하는 데 많은 시간과 자원을 소모하고 있습니다.
- 또한 0.74%에 해당하는 취약점이라 하더라도, 그 모든 취약점이 귀사의 환경에서 실제로 악용 가능한 것은 아닙니다.



P.29 - The Filter — From Prioritization to Confirmation
The Broken Physics of Remediation, Research Report from Qualys TRU

초(超)우선순위 설정의 필요성

악용 가능 ≠ 실제 악용 가능

우선순위가 지정된 노출(취약점) 중 보완 통제(Compensating Controls)를 우회하여 실제 악용 가능한 것은 20% 미만입니다.

자사 환경에서의 실제 악용 가능성을 검증하면 필요한 대응 조치 수를 줄일 수 있습니다.

리스크 관리 현황

Dashboard Tourism

오늘날 우리는 모두 **‘리스크 두더지 잡기’** 게임을 하고 있는 것 같습니다.

공격 표면 관리에서 리스크 표면 관리로

ROC

리스크 운영 센터를 소개합니다

ETM: ROC의 동력

885 Critical
TruRisk™ Score







Unified Asset Inventory → **Risk Factors Aggregation** → **Threat Intelligence** → **Business Context** → **Risk Prioritization** → **Risk Response Orchestration** → **Compliance & Executive Reporting**

Security and Risk Findings | Risk Identification

(Built in threat intel feeds, enriched with in-house vuln research)

(CMDB, Custom Data Sources)

QUALYS

- Vulnerability
- App Security
- Configuration
- Asset Management
- Compliance
- Attack Surface
- Cloud Security
- AI Security

NON-QUALYS

- Vulnerability Management
- Compliance
- Runtime Security
- Application Security

THREAT INTELLIGENCE

packet storm, McAfee, FIREEYE, MISP Threat Sharing, IMMUNITY, GitHub, CANADIAN CENTRE FOR CYBER SECURITY, REVERSING LABS, Qualys Vulnerability Research Team, PZ PROJECT ZERO, VDE, Kaspersky Industrial CyberSecurity, MITRE ATT&CK, EPSS, Talos, Square Security, GREYNOISE

BUSINESS CONTEXT

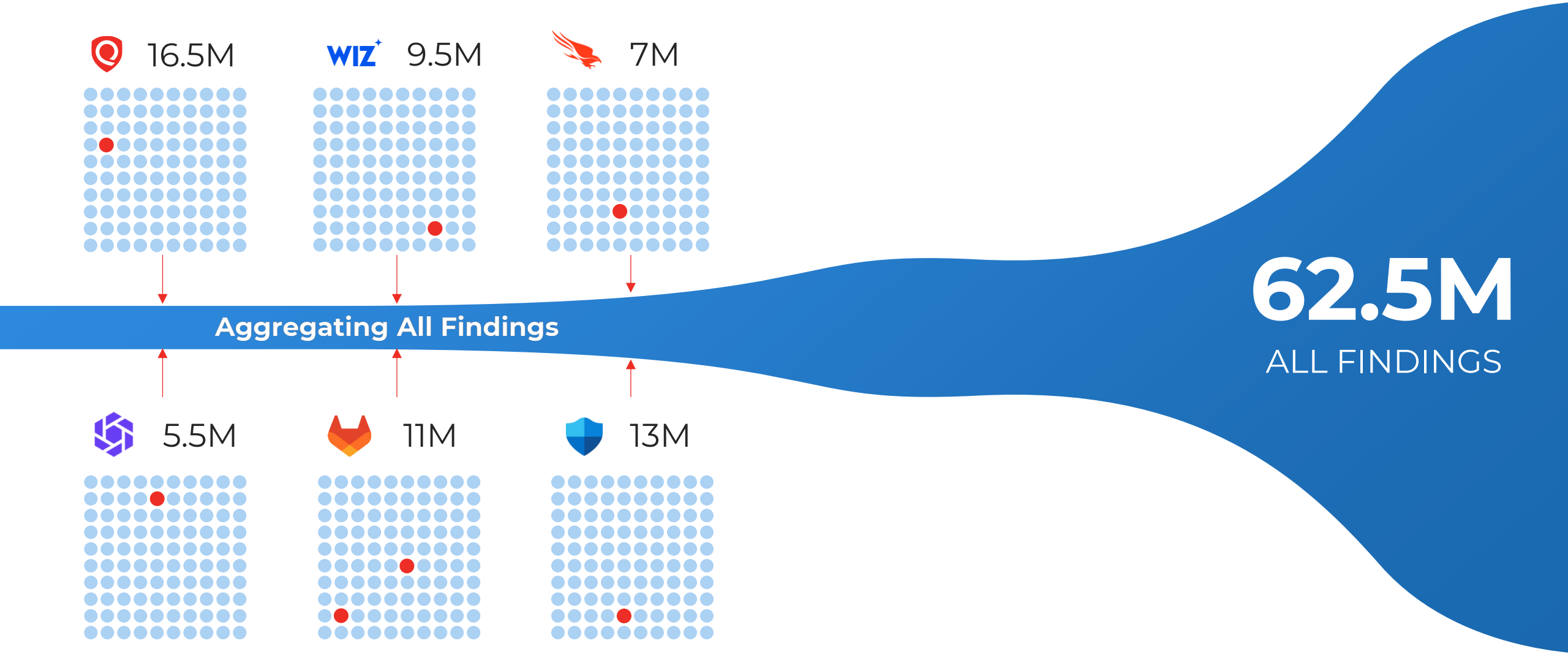
CMDB, GRC, Active Directory

MEASURE | Quantify Cyber Risk in Business Terms

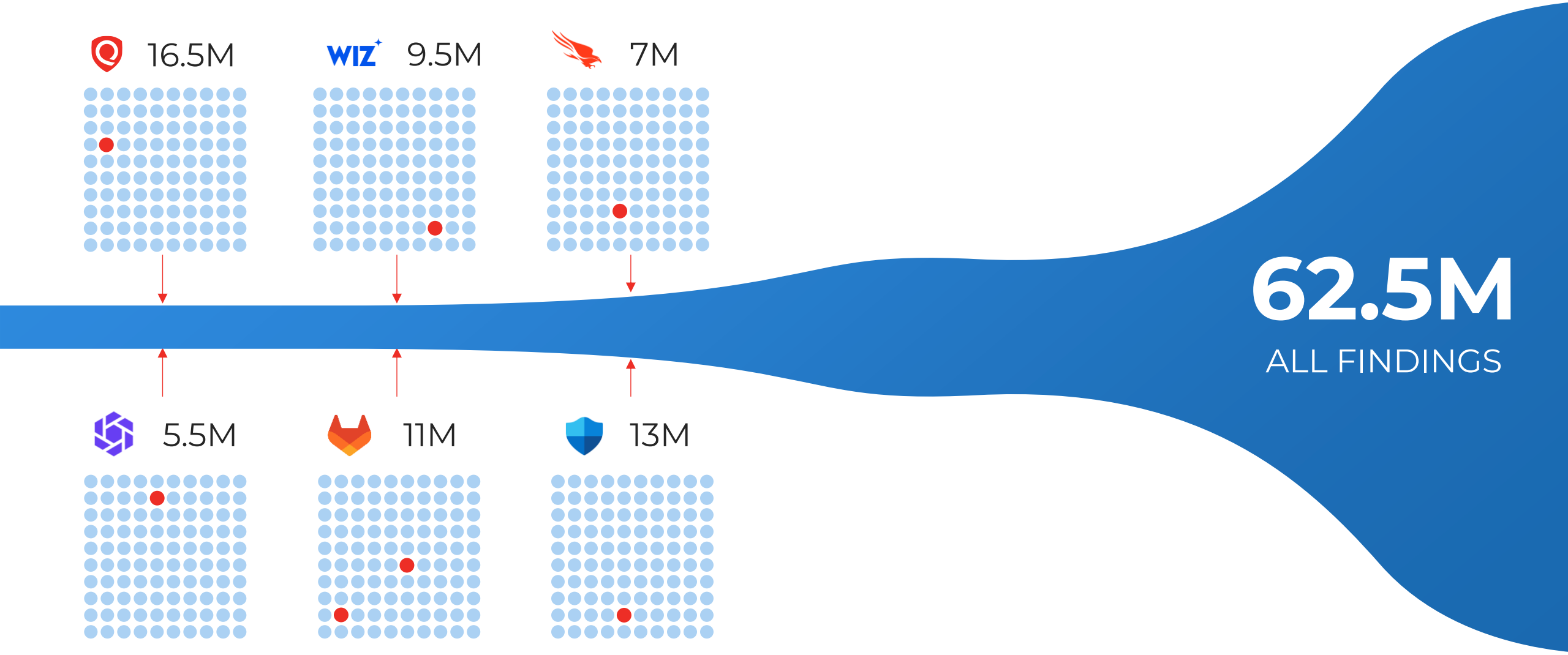
COMMUNICATE | Executive Reporting and Ticketing

ELIMINATE | Patch Mitigate & Track

수백만 개의 파편화된 노출이 하나로 모여들다

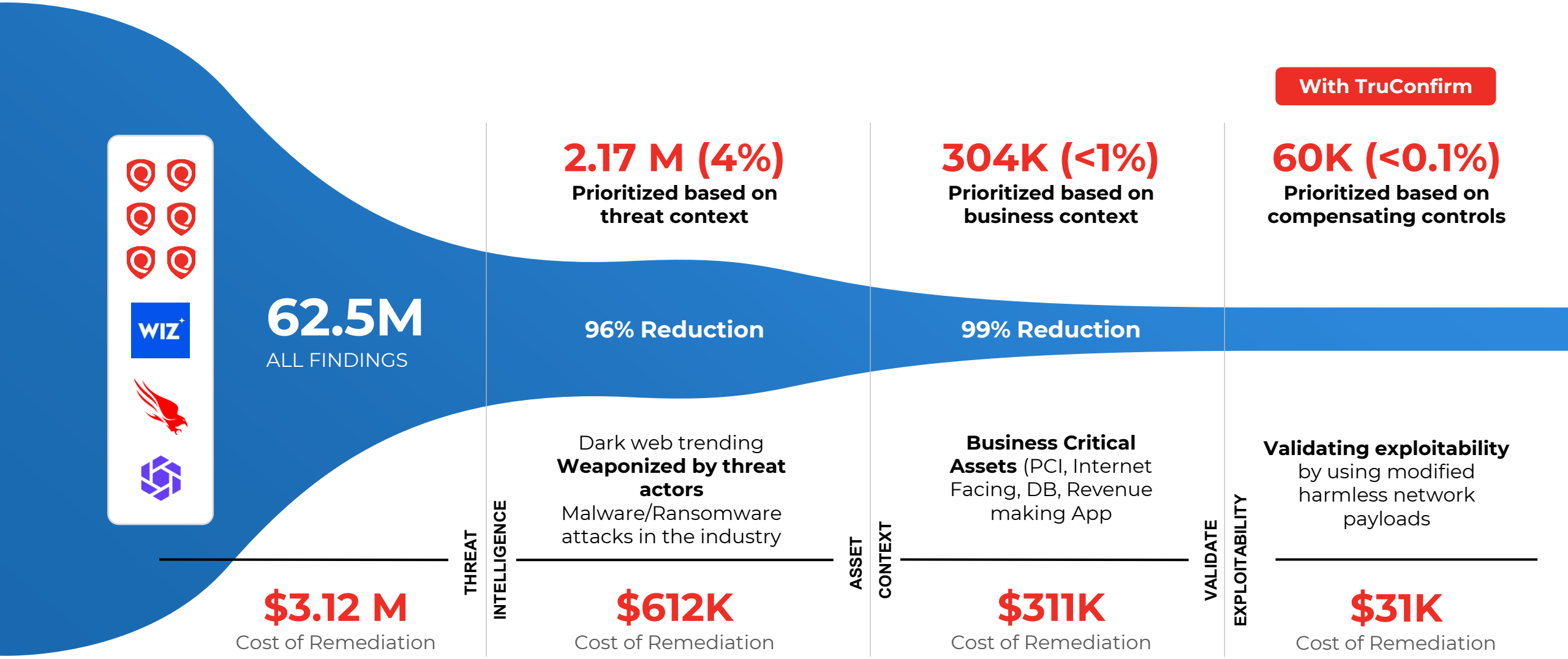


수백만 개의 파편화된 노출이 하나로 모여들다

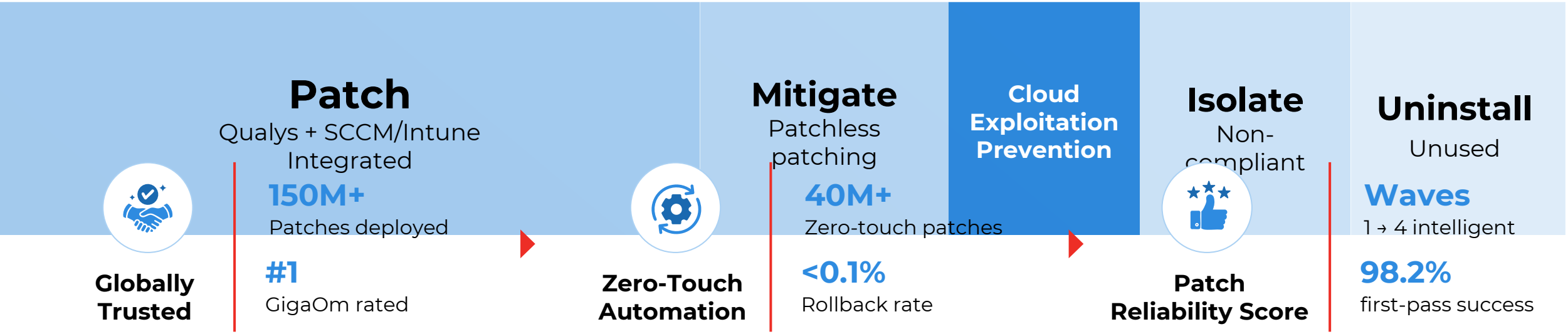


중요한 리스크를 우선순위에 두면 효율성이 높아집니다.

Risk Operations Center (ROC)



TruRisk Eliminate
패치 적용 여부와 관계없이 위험 제거



에이전트형

AI ROC

Your skilled, digital workforce for autonomous risk management

취약점의 자율적 해결
Qualys AI-ROC 기반

제로데이 취약점 조치

- 패치 및 설정변경을 통한 대응방안 제공
- 운영 안정성을 보장하는 자동화 기능 제공

Agent Sara

초(超)우선순위화

- 위협 수준, 비즈니스 영향도 및 자산 중요도를 기반으로 우선순위 결정
- 기존 보안 통제를 고려하여 실제 악용 가능성 검증

Agent Val

AI 수준 초고속 탐지

- 취약점 공개 즉시 탐지
- 온프레미스, 클라우드, 애플리케이션 및 컨테이너 전 영역에 대한 가시성 및 보호 제공

Agent Insta

Qualys 플랫폼 AI 전략: 다중 모델

Use Case Driven to Maximize Reasoning Power and Cost-Efficiency

Models integrated on platform for Agentic AI Tasks

- Open-source models *(Llama, Mistral)*
- Customized SLMs *(Phi-4 Mini from Microsoft)*
- LLMs from Anthropic *(Claude Haiku / Sonnet / Opus)*

Models for Internal Use for Threat Research & Defense

- Anthropic's Glasswing & Cyber Verification Program (CVP)
- OpenAI's Trusted Access for Cyber (TAC)
- Evaluating frontier models from other labs

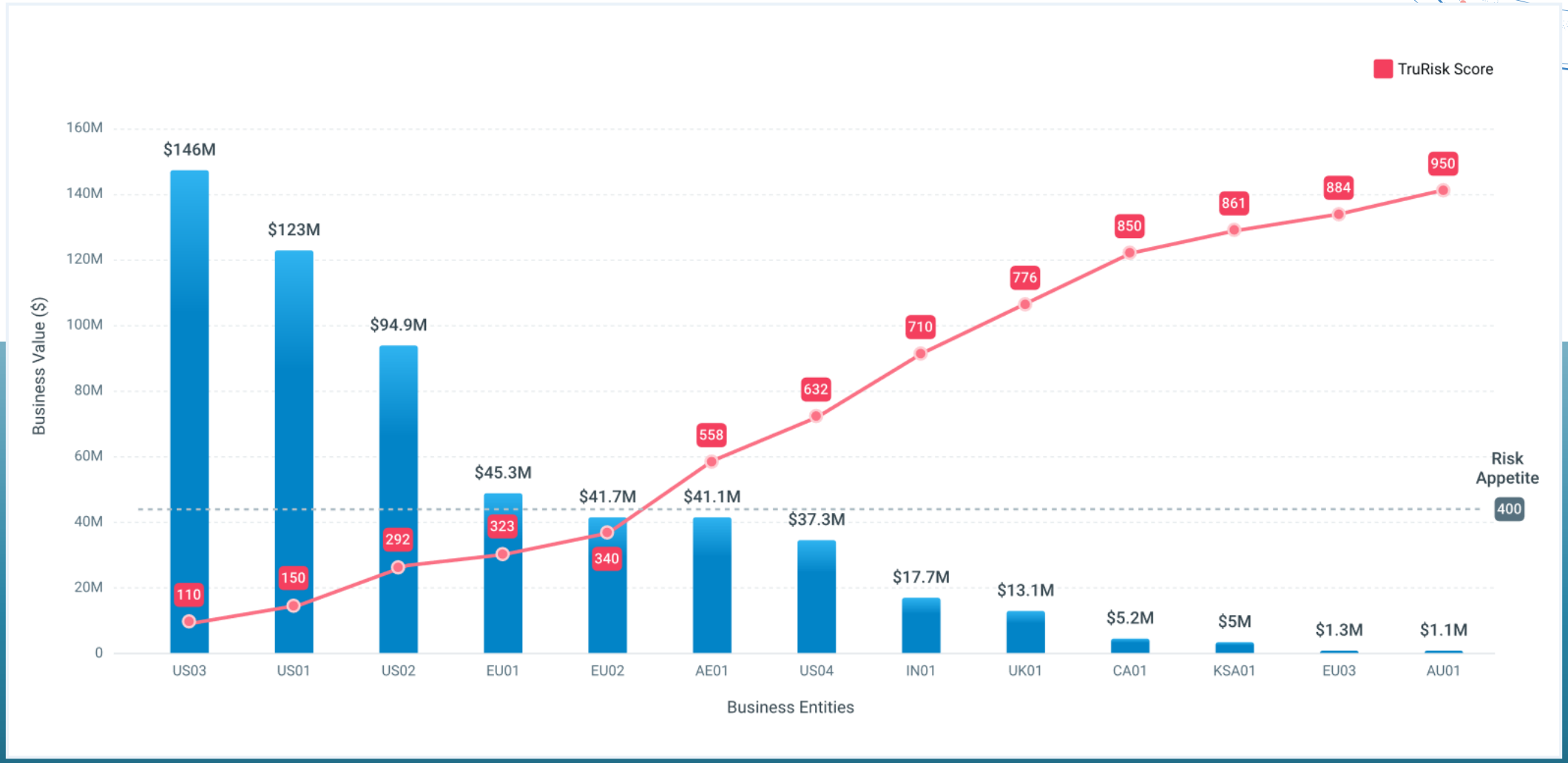
Integrations with Models for SAST Use Cases

- Import findings in customer source code into Qualys ETM
- Apply runtime context for prioritization with Qualys
- Patch or mitigate prioritized vulnerabilities

ANTHROPIC Mistral AI OpenAI Microsoft Meta

리스크 관리는 기업이 직면할 수 있는 막대한 재정적 손실의 가능성을 줄여가는 방향으로 구성됩니다.

ROC는 사이버 리스크를 비즈니스와 연계합니다.




감사합니다.