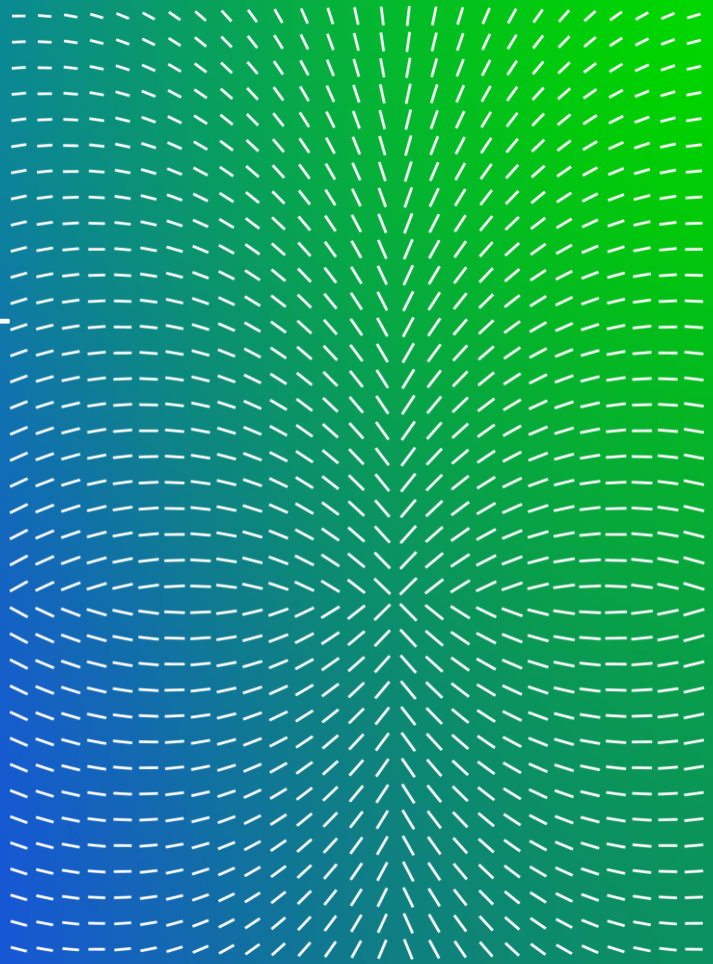
Trellix

트렐릭스 보안 플랫폼, 진화하는 위협에 대한 근본적 대응

김 현섭 기술총괄

Trellix Korea



Trellix Platform

- Endpoint Security
- Data Security
- Cloud Security
- Email Security
- Network Security
- 3rd Party Engine

XConsole

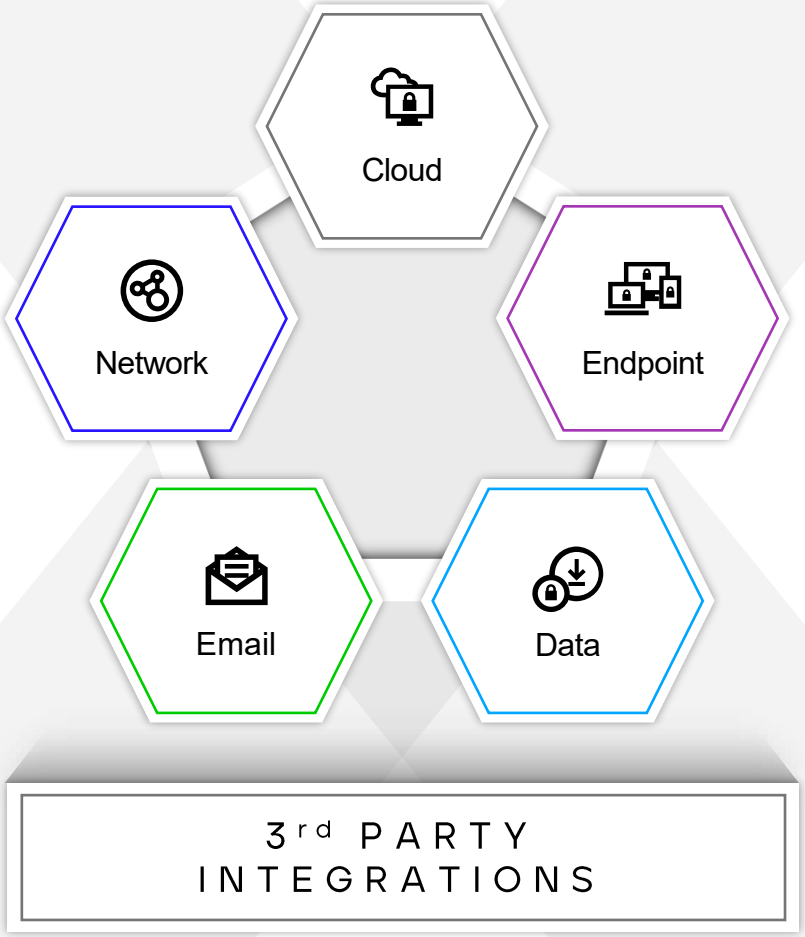
Core Engines

Advanced Research Center

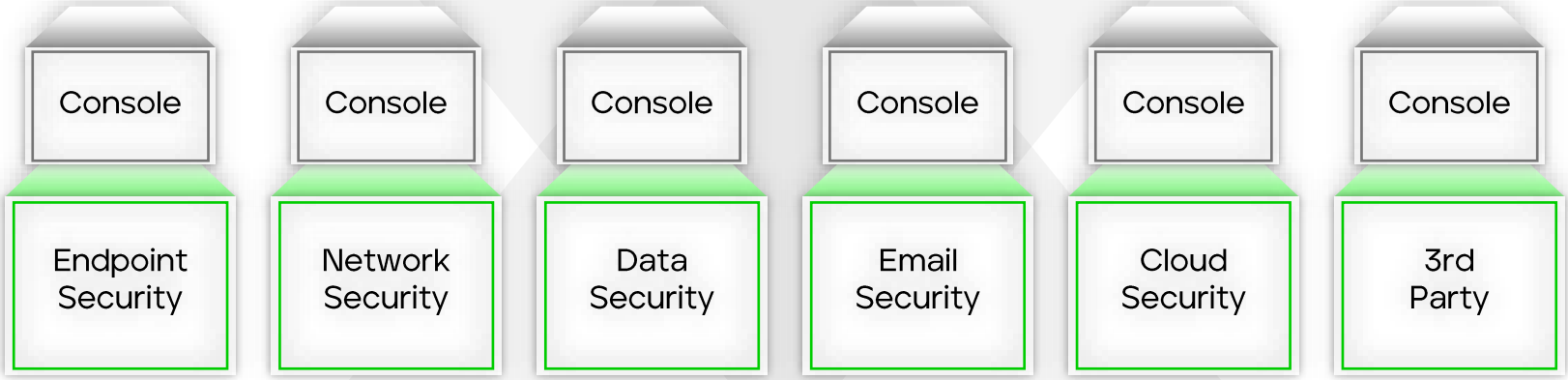
Data Lake

- Product Research
- Threat Intelligence
- Adversarial Resilience & Advocacy
- Data Science ML / AI
- Research Engineering

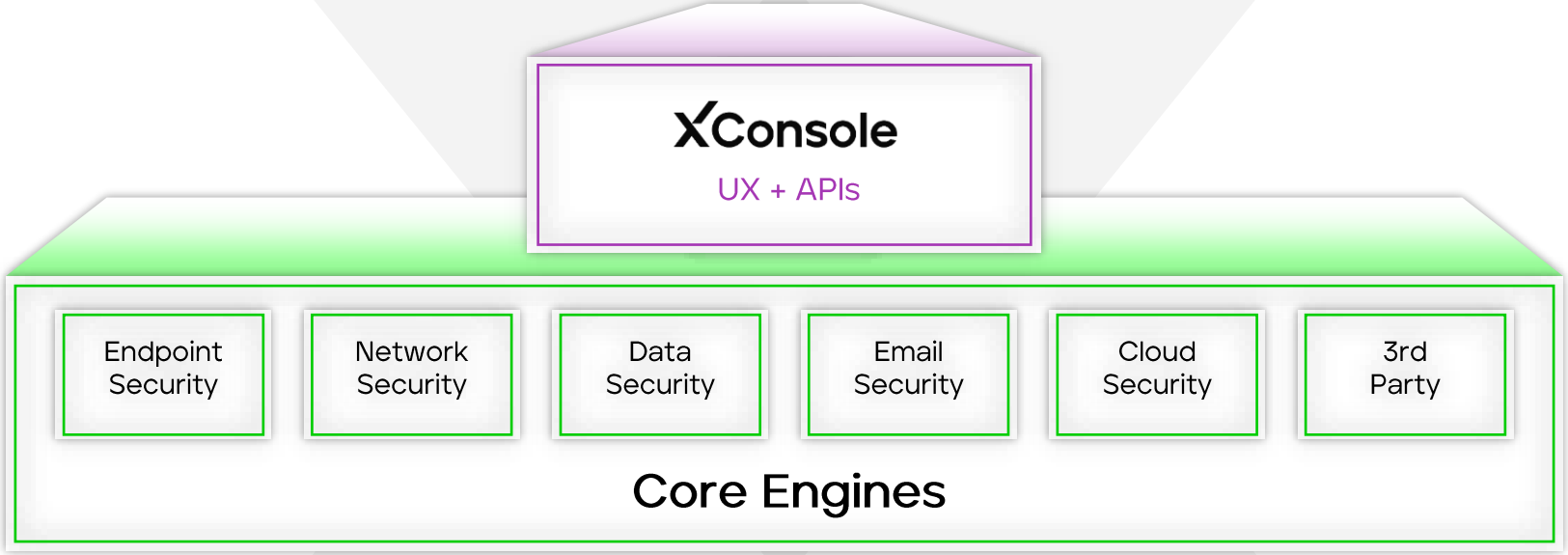
Trellix Product Lines



Trellix


Console
Endpoint Security
Console
Network Security
Console
Data Security
Console
Email Security
Console
Cloud Security
Console
3rd Party

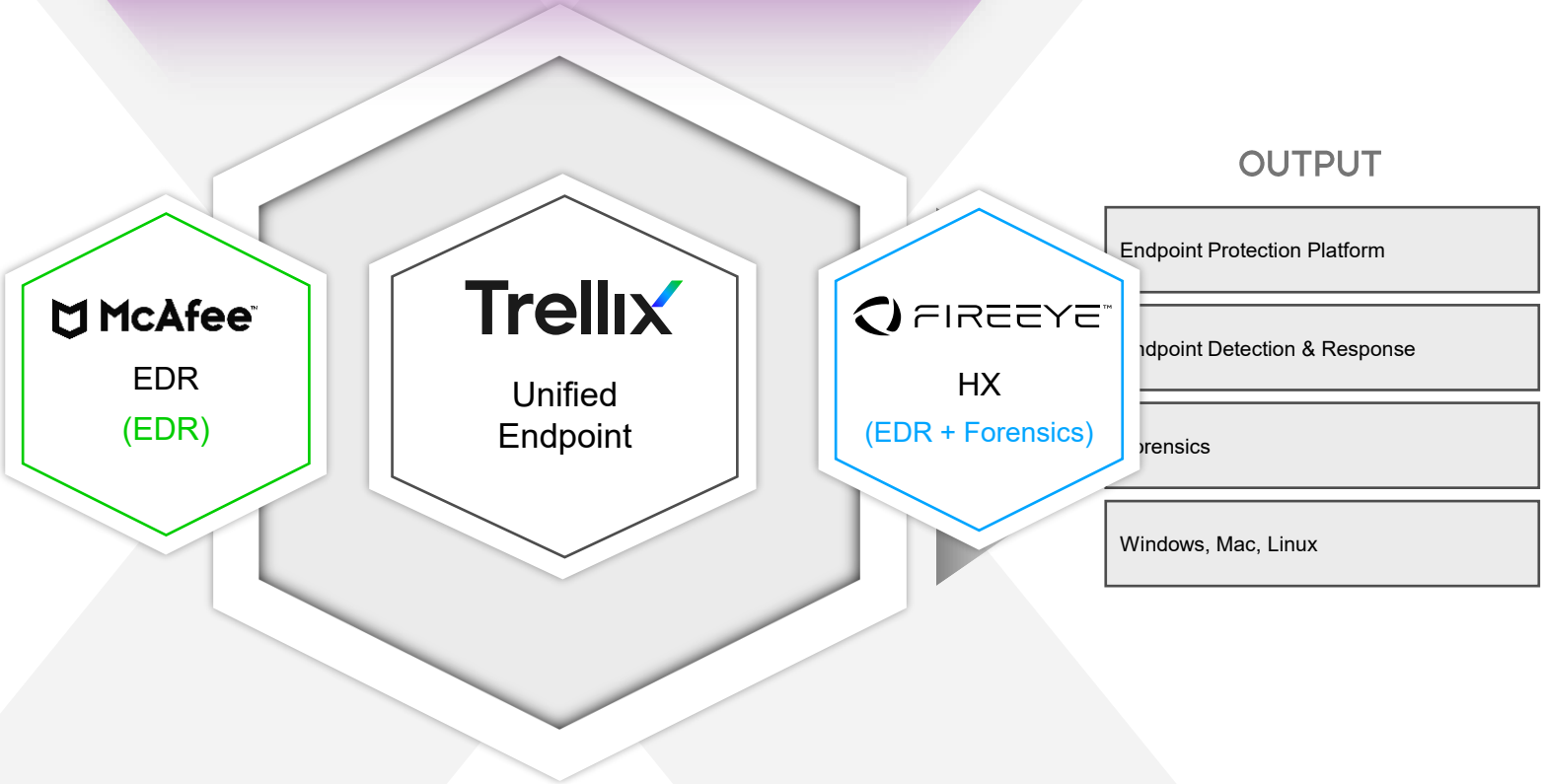
Trellix


XConsole
UX + APIs
Endpoint Security
Network Security
Data Security
Email Security
Cloud Security
3rd Party
Core Engines

Trellix

NEW

XConsole

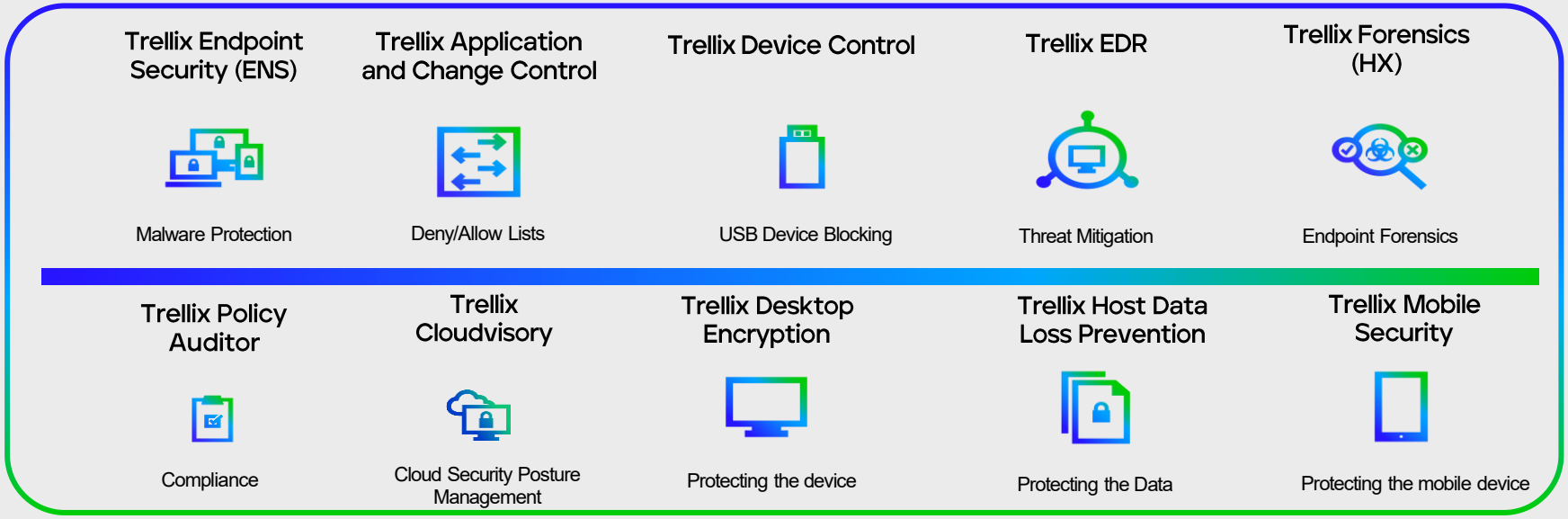


OUTPUT

- Endpoint Protection Platform
- ndpoint Detection & Response
- orensics
- Windows, Mac, Linux

Trellix

Trellix Endpoint Security



Trellix

Trellix Unified Security

e Policy Orchestration

NEW

BETA : Q4

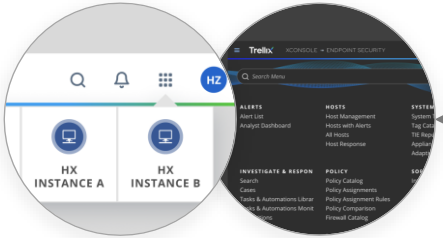
Trellix Agent (TA)

Endpoint

Trellix Endpoint Security (ENS)	Trellix Application and Change Control	Trellix Device Control	Trellix EDR	Trellix Forensics (HX)
Malware Protection	Deny/Allow Lists	USB Device Blocking	Threat Mitigation	Endpoint Forensics

Trellix Policy Auditor	Trellix Cloudvisory	Trellix Desktop Encryption	Trellix Host Data Loss Prevention	Trellix Mobile Security
Compliance	Cloud Security Posture Management	Protecting the device	Protecting the Data	Protecting the mobile device

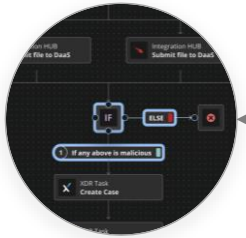
XConsole / Endpoint 단계별 연동



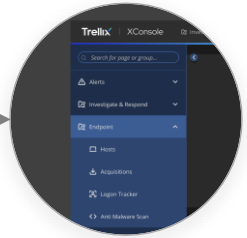
Access Apps
via App Switcher

Navigate
Mega Menu

EDR & EPO Workflows
with XC Styling



Native XC
Workflows



XC Side Nav Replaces
Mega Menu (Timing TBD)

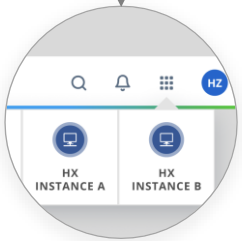
XConsole 1

XConsole 2

Endpoint 1.1

Endpoint 1.2

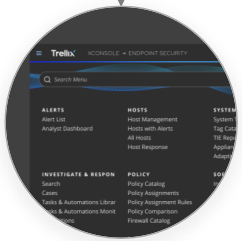
Endpoint 2.0



Access Endpoint
via XC App Switcher

Navigate Endpoint
Via Legacy HX Nav

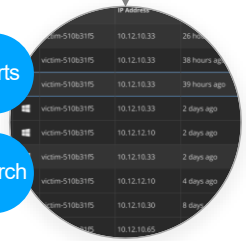
Legacy HX
Workflows



Navigate
via XC Mega Menu

HX Adopts
Muse Styling

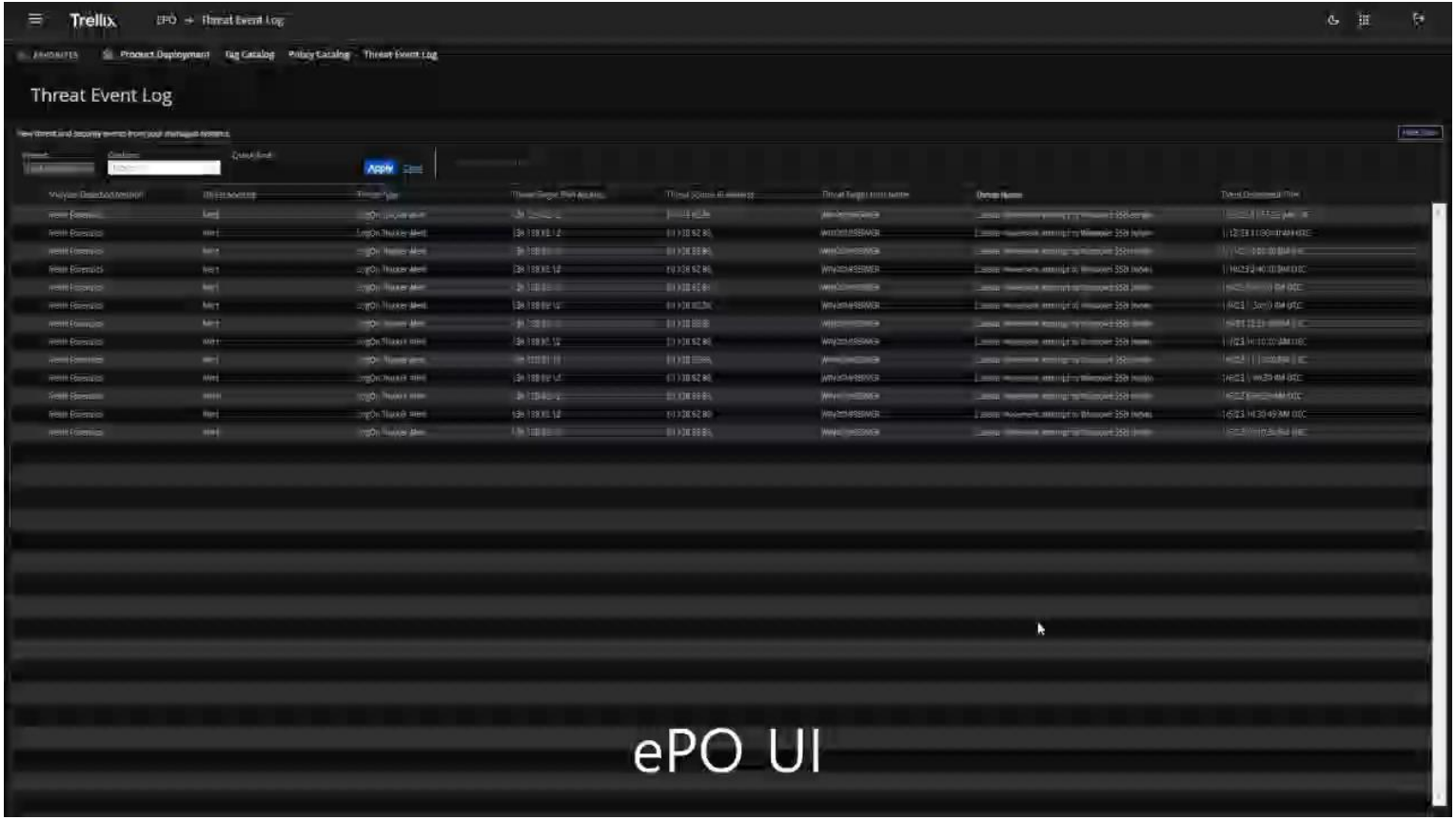
Access & Navigate
via XC Side Nav



HX Workflows Migrate /
Integrate to XC Native

Trellix

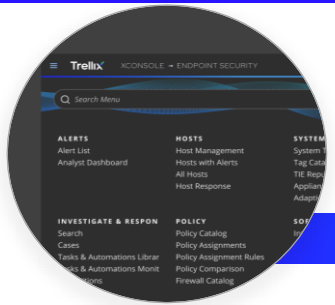
Trellix Unified Endpoint Security Experience



Trellix

Trellix
Network / Email Security

Trellix

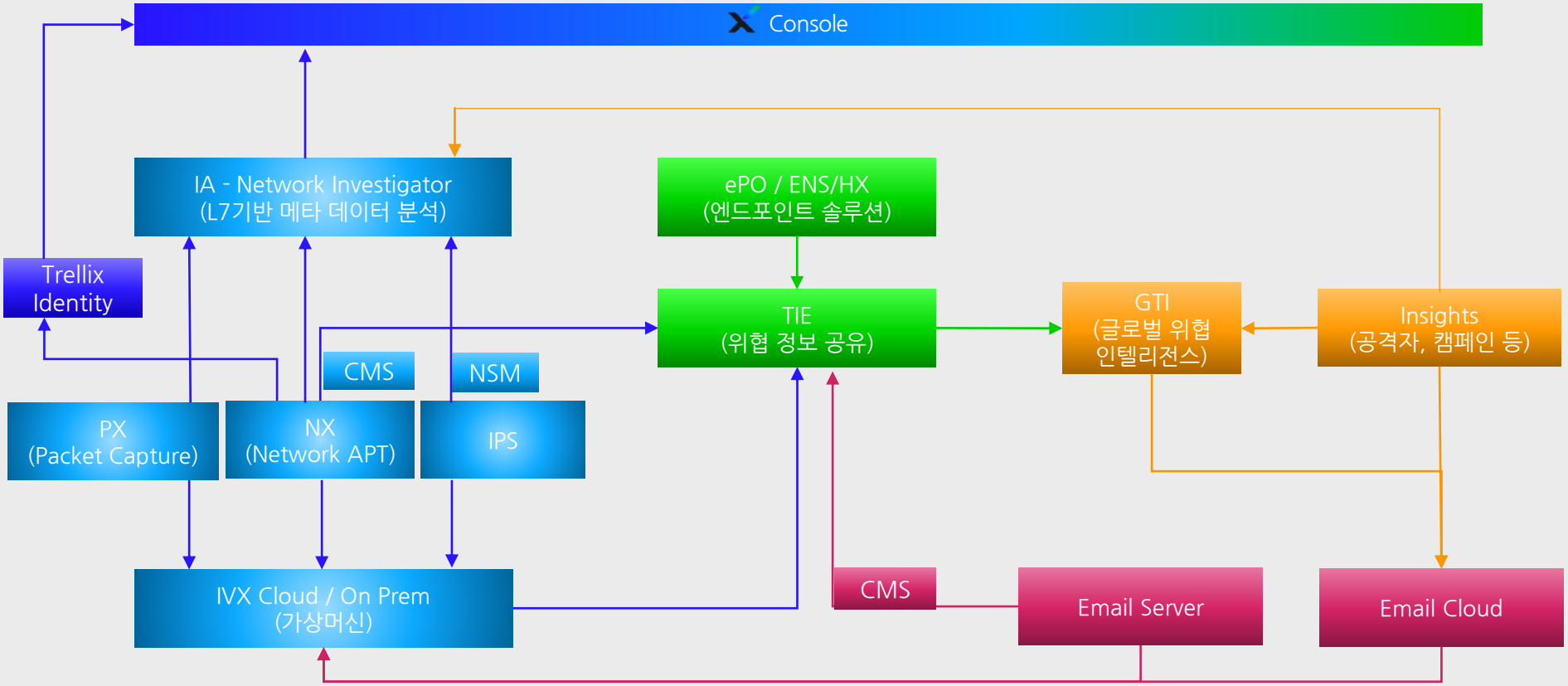


Console

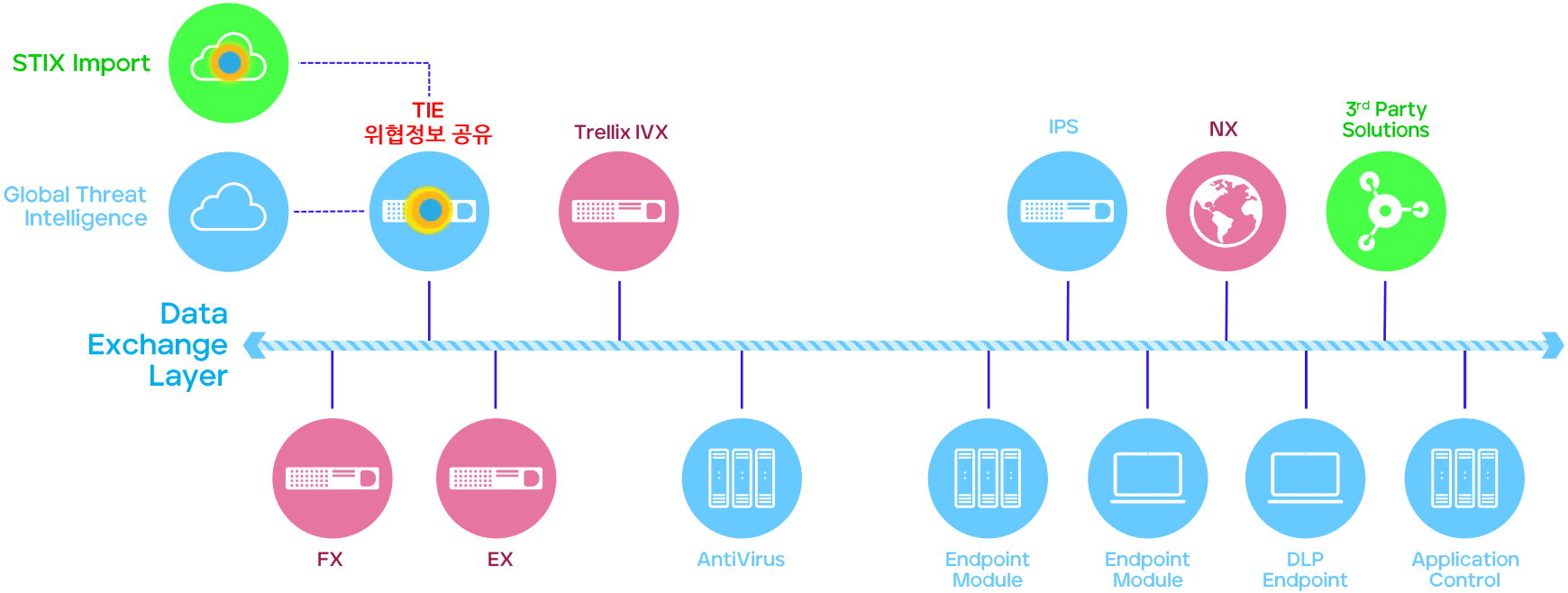
Trellix

NEBU Portfolio

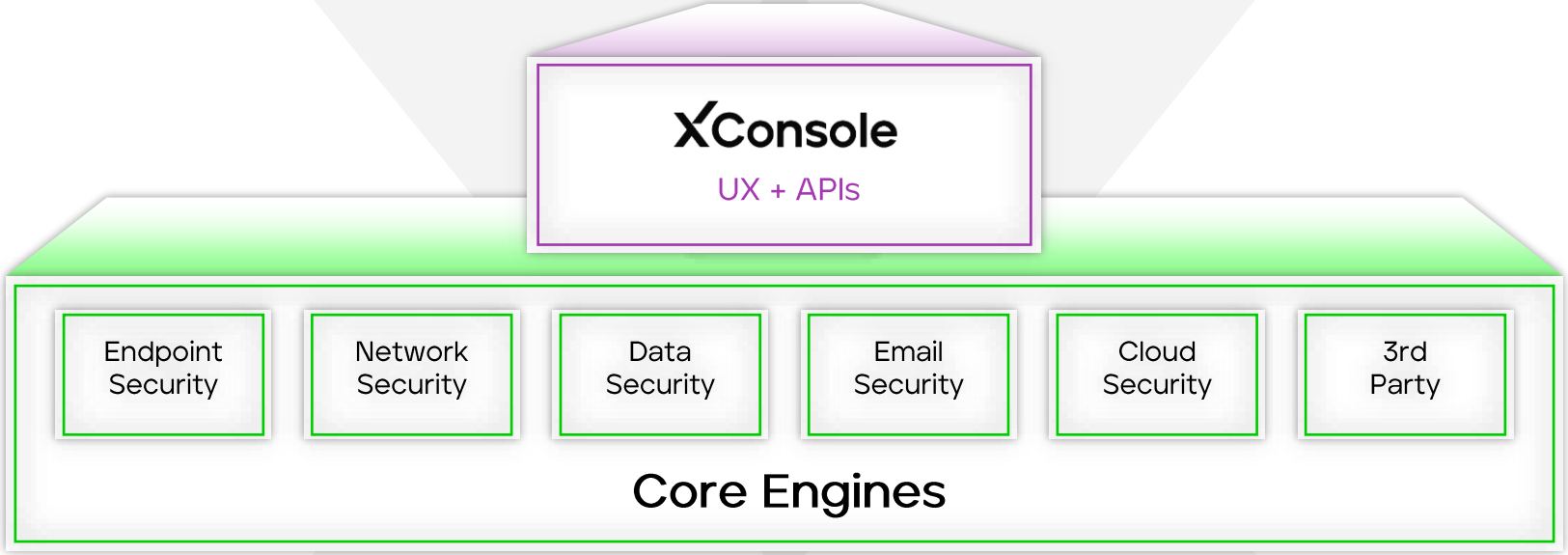
포트폴리오 전반에 걸쳐 통합



기업 내에 위협 정보 교환 모델 (TIE)

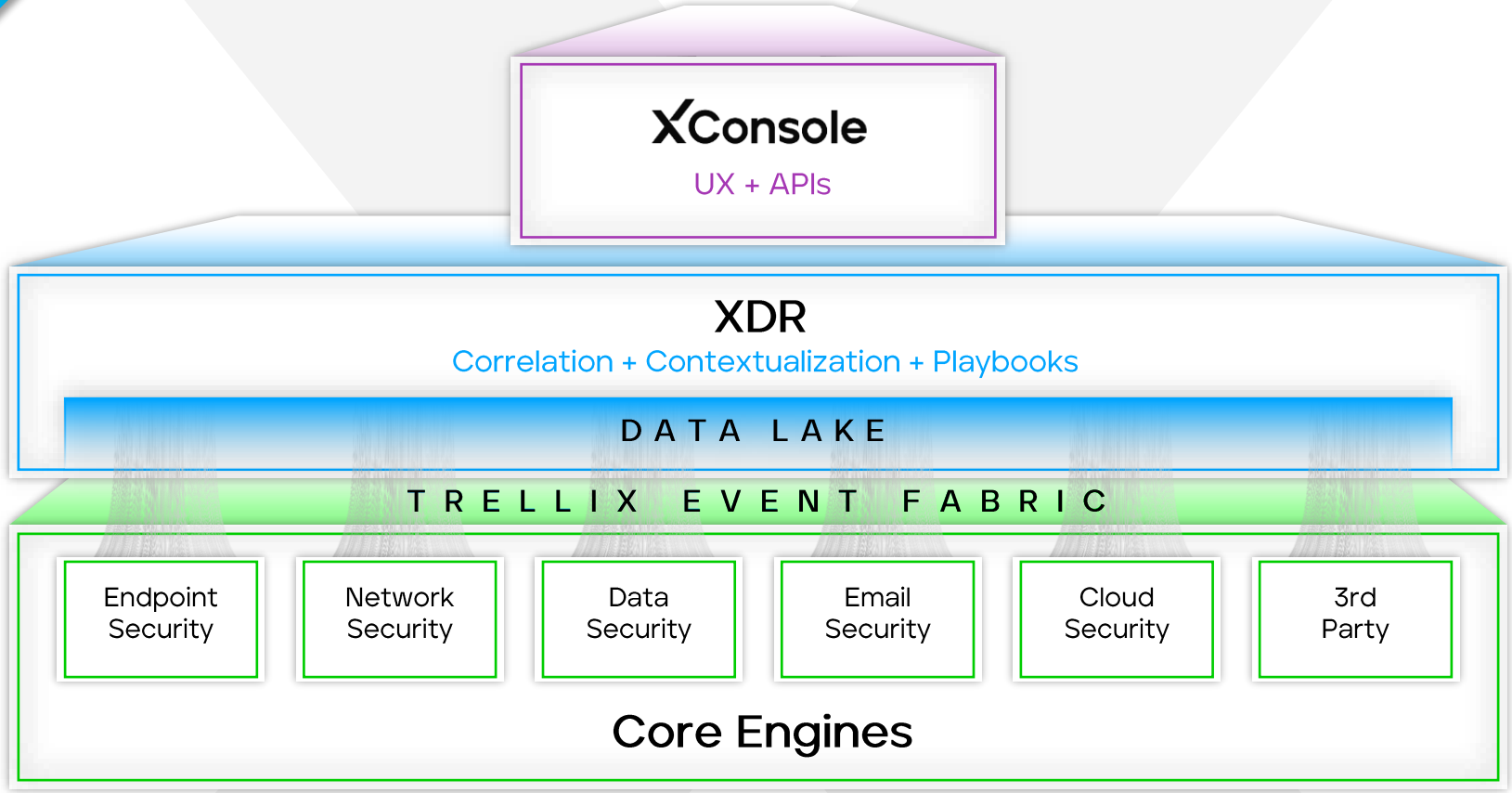


Trellix


XConsole
UX + APIs
Endpoint Security
Network Security
Data Security
Email Security
Cloud Security
3rd Party
Core Engines

Trellix

NEW


XConsole
UX + APIs
XDR
Correlation + Contextualization + Playbooks
DATA LAKE
TRELLIX EVENT FABRIC
Endpoint Security
Network Security
Data Security
Email Security
Cloud Security
3rd Party
Core Engines

Trellix

Trellix

Open & Native

TRELLIX Products portfolio

IT/SecOps Researcher Partner MSSP

XConsole

UX + APIs

- NG SIEM & SOAR capabilities
- Threat Intelligences (Insights & Mandiant & Intel 471)
- Advanced Analytic, AI, ML Engine

Trellix XDR Platform

Correlation + Contextualization + Playbooks

Trellix ADVANCED RESEARCH CENTER

- Knowledge services

DATA LAKE

TRELLIX EVENT FABRIC (API)

Core Engines

TRELLIX Products portfolio

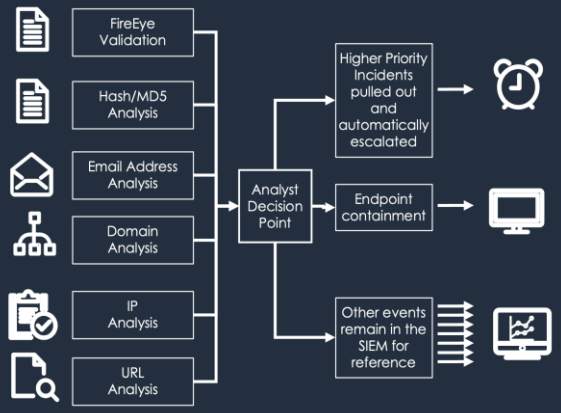
Endpoint Security	Network Security	Data Security	Email Security	Cloud Security	3rd Parties
• End Point Security • EDR • Forensic	• Network Security (NX) • Network IPS (NSP) • Network Forensic (PX) • Sandbox (IVX)	• Device Control • Encryptions • Enterprise DLP (eDLP, nDLP, Gateway DLP, Cloud DLP)	• Advanced Email Security / APT (On-Premise & Cloud) • Sandbox (IVX)	• Sandbox (IVX & DaaS) • Skyhigh Security • SIEM/HELIX/ePO	100+ Vendors 200+ Plug-ins 650+ Parsers 75+ Cloud Connectors
Trellix Unified EndPoint Security Platform	Trellix Network Investigator (NDR)	Trellix ENT DLP Solution	Collaboration Security	Security Operations	

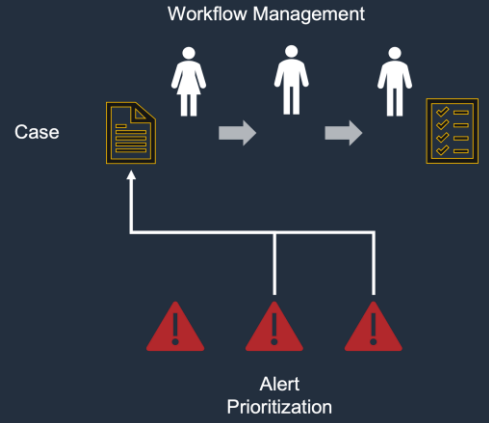
- Atlassian Jira
- AWS GuardDuty
- CB Endpoint
- Cisco Umbrella
- IBM Qradar
- Netskope
- Okta
- Palo Alto Prisma
- ThreatQ
- ServiceNow
- Sync Bluecoat
- Windows Defender

탐지/분석 대상의 확대

통합 보안 운영 프로세스 제공 (보안 운영 플랫폼)

로그 수집 > 자동화 > 실시간 탐지 > 우선순위 > 분석/조사 > 대응/조치



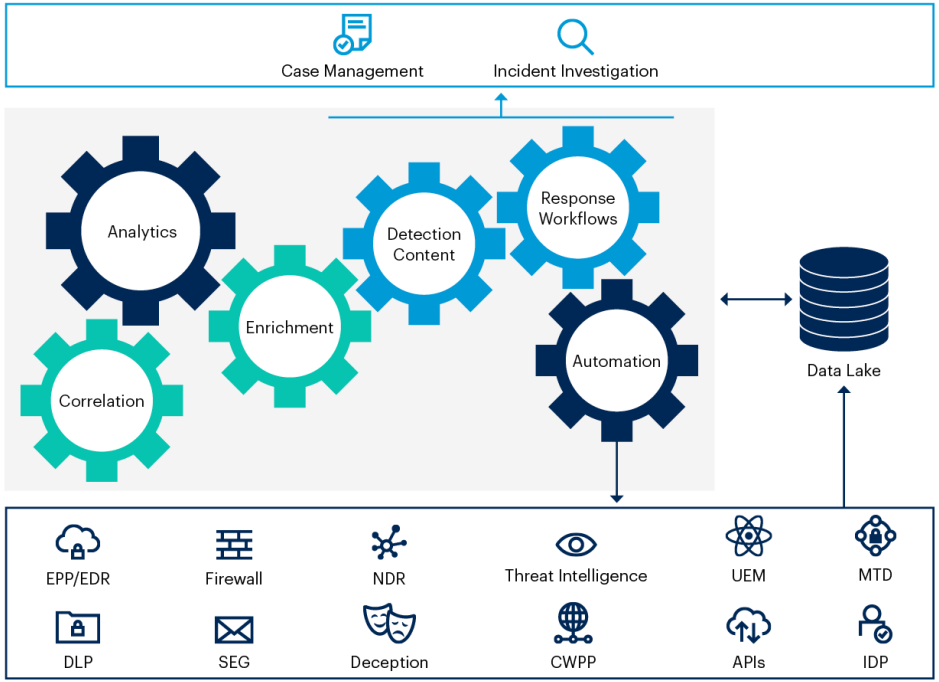


Trellix

Gartner - XDR Market Guide 2023

https://www.gartner.com/doc/reprints?id=1-2EOYTQA6&ct=230811&st=sb

XDR Core Elements



Source: Gartner
761828_C

Gartner

XDR이 제공하는 전반적인 효과

- 다양한센서로부터 고급 분석을 사용
- 인시던트를 탐지하고 해결하는 데 걸리는 시간을 대응 가능한 수준으로 단축.

분석 및 자동화 대응

- 통합 정책엔진(Unified policy engine)
- API를 통한 타사 제품과의 통합
- 고급 분석 제공
- 분석가를 위한 자동화, 오케스트레이션, 워크플로우 기능을 자체적으로 수행할 수 있는 기능
- 위협을 감지 및 처리하여 이벤트를 상호 연관시키고 여러 신호에서 워크플로우를 개선

센서/응답

- XDR 제품은 최소 2개의 기본 보안 센서를 제공해야 하며, 이 중 하나는 엔드포인트가 포함되어야 함
- 로그 수집은 필수

기존 구축된 통합을 통해 보안 제품을 단일 공급업체로 통합

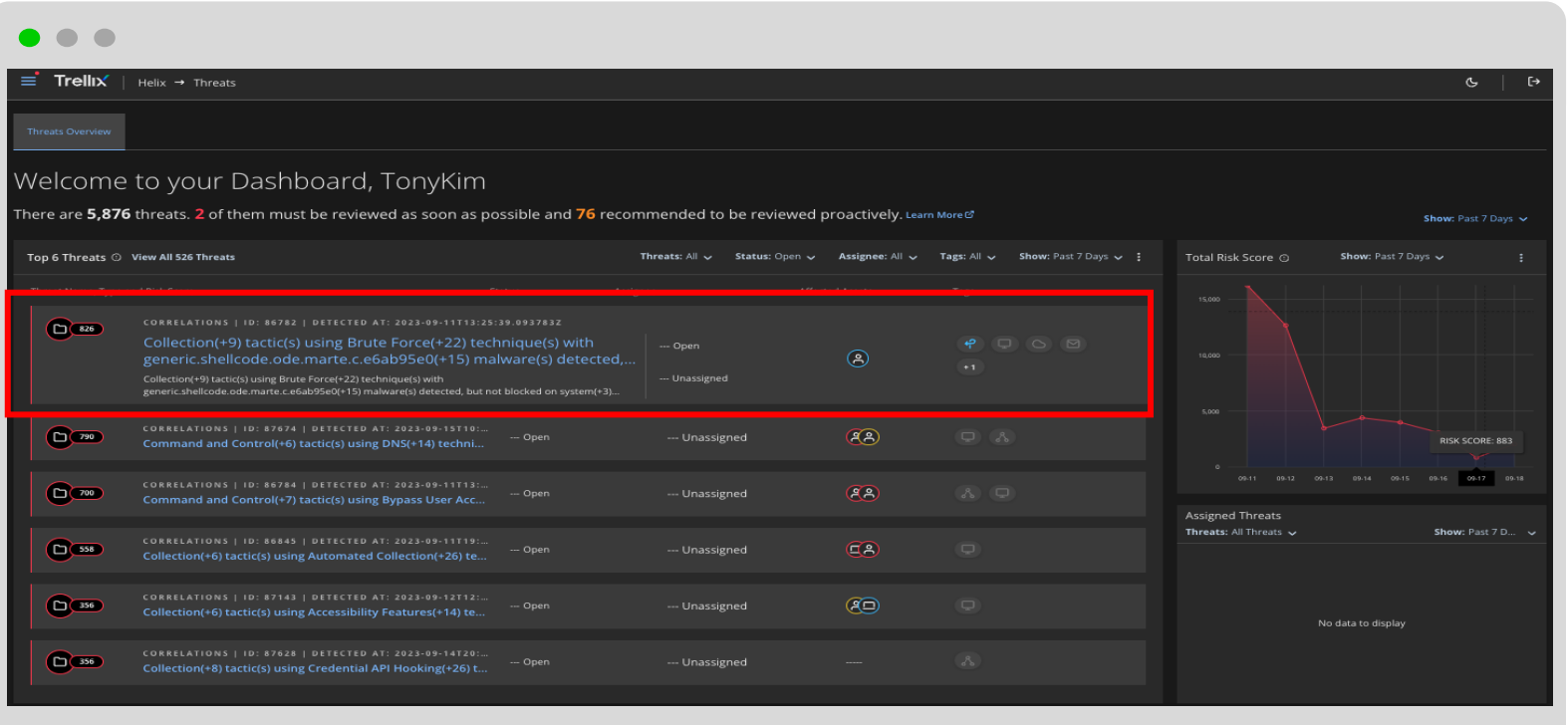
Gartner Use Case 1

1000+ Integrations:

- Cloud IaaS • Cloud SaaS • Identity • Firewall • Proxy • Network Infrastructure • OS • Apps
- 3rd party Endpoint Security • Email Security • Network Security • Data Protection • Cloud Security
- 3rd party Threat Intelligence

Operationalizing Threat Intelligence

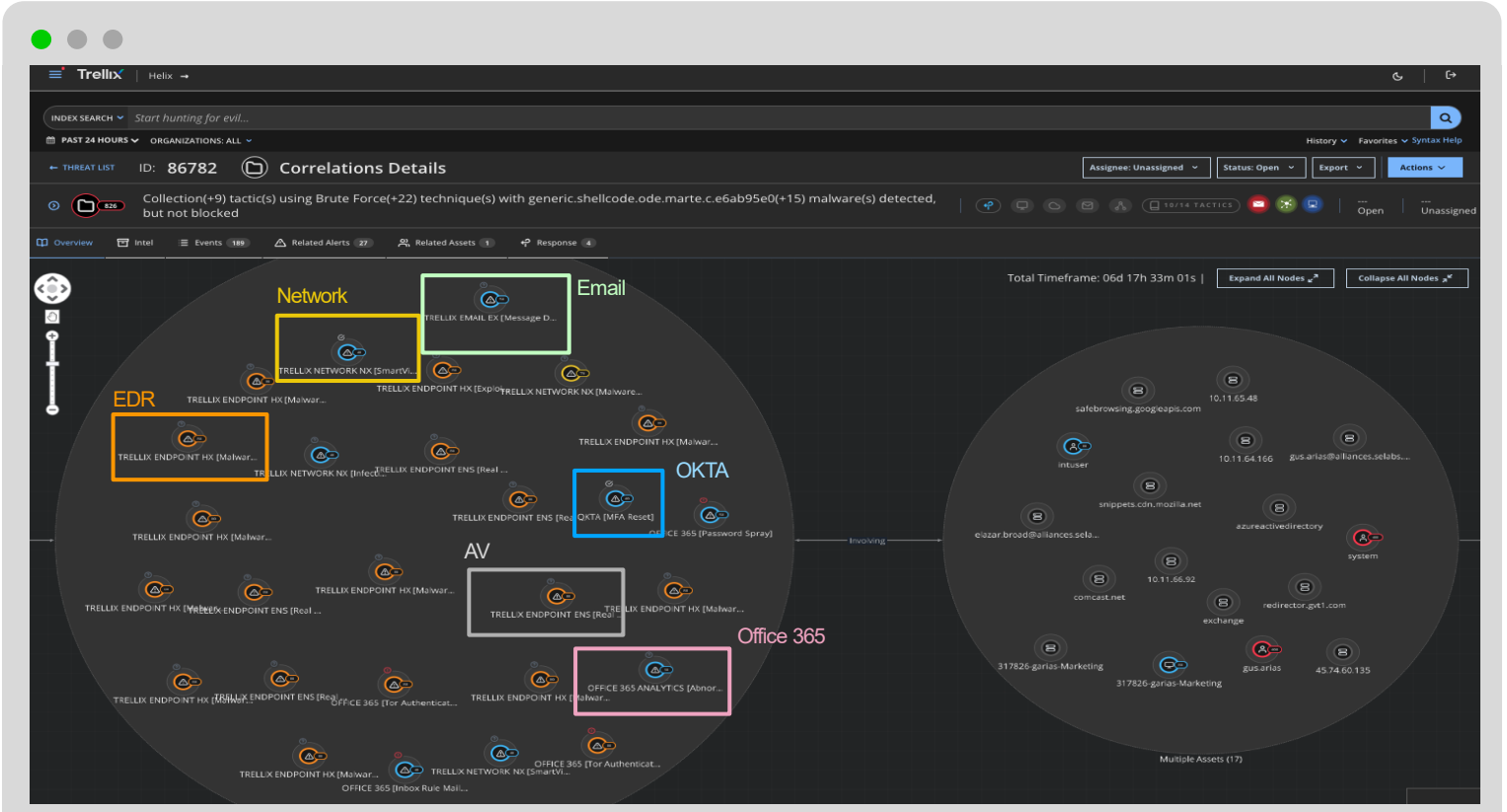
Gartner Use Case 2



다양한 보안 제품과 결합된 탐지 효율성 향상 및 대응

Gartner Use Case 3

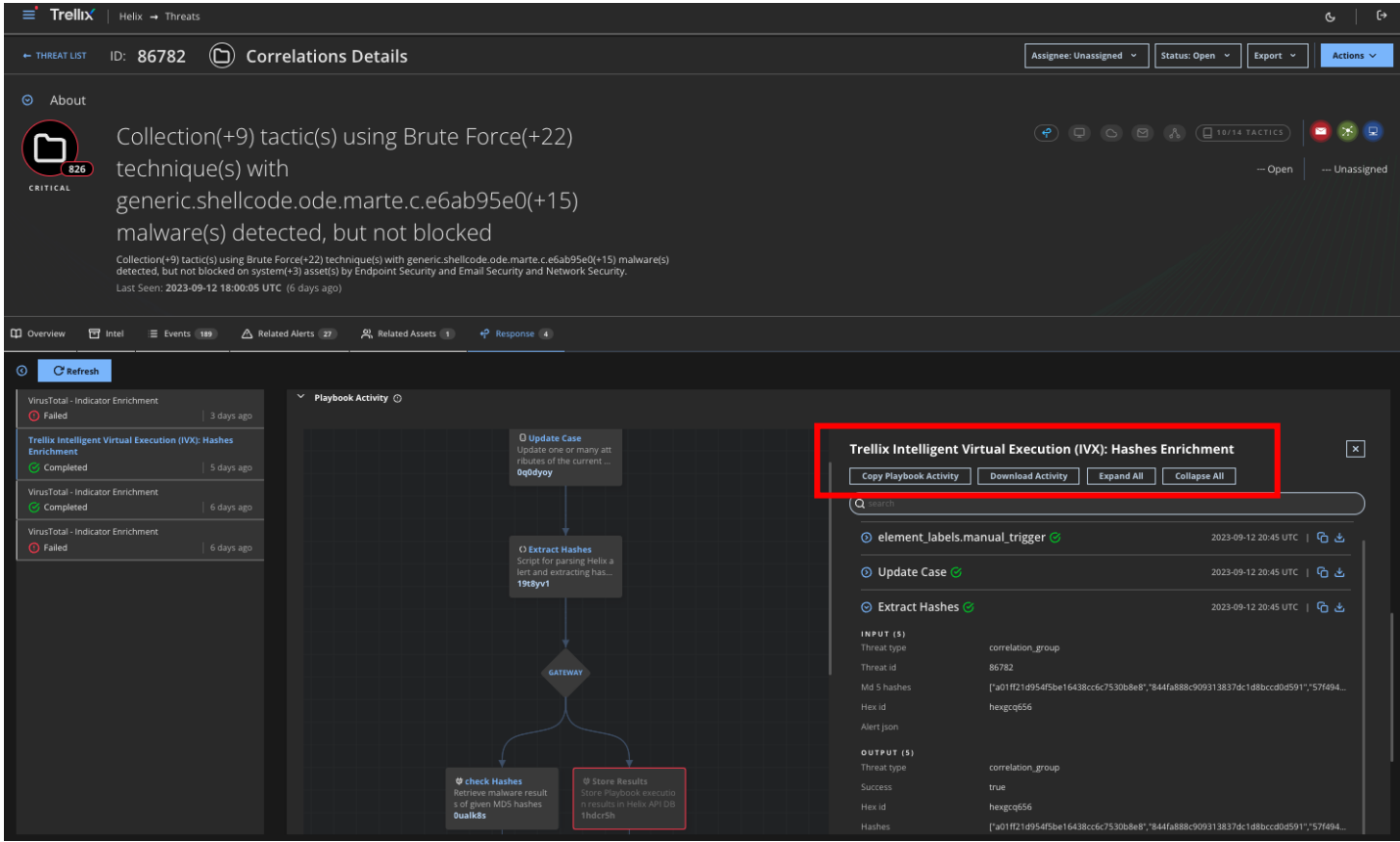
- 웹, 엔드포인트 및 인텔리전스와의 상호 연관성
- 이벤트와 연관된 자산에 대하여 쉽게 확인
- 스토리보드 확대 및 축소



탐지 및 대응 플랫폼의 기본 제공 자동화 기능 극대화

Gartner Use Case 4

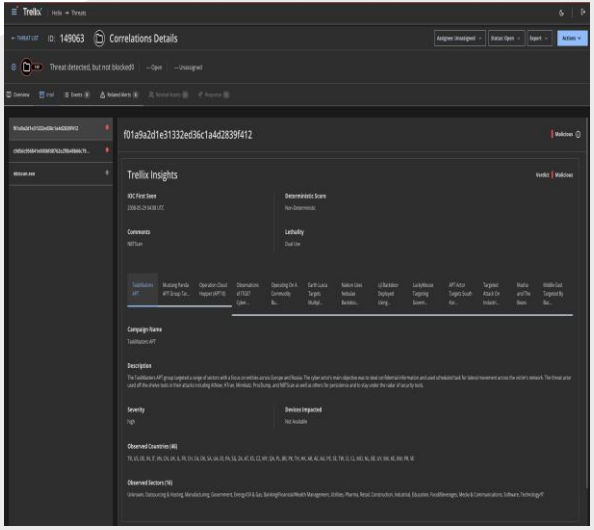
- 조사 강화에서 격리까지 다양한 플레이북 제공
- 더 좋은 의사 결정을 안내하는 전문 지식 제공
- 작업 진행 및 완료 상태

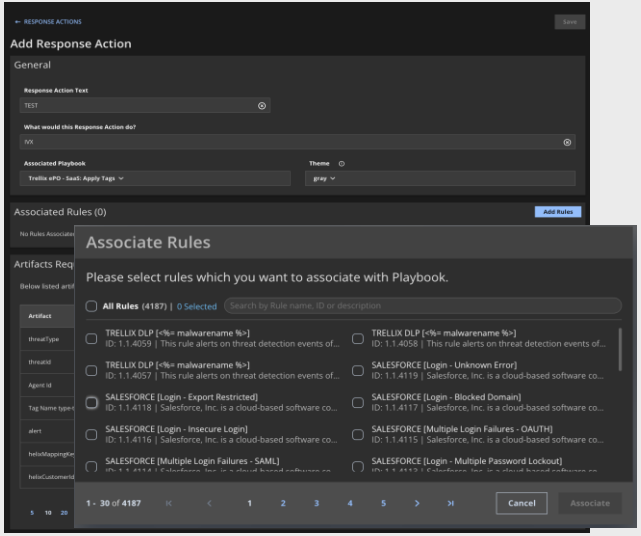


XDR Journey and Beyond

Fully Capable XDR

- Multi data source integration
- Cross source correlation (multi-vendor, multi-vector)
- Integrated playbooks and response actions
- Trellix threat intel





Simplified XDR

Low Code SOAR

- Simplified low code approach to orchestration and response

SecOps UX 강화

- New Alerting, Search & Forensics, Rule Mgt, Case Mgt, Tasks & Playbooks Apps
- Guided, Persona based UX

통합 확대

- Broadened data Integrations and Response actions
- Easily integrate Trellix Products

New XDR Cross Vector Detections

Thank You

Trellix