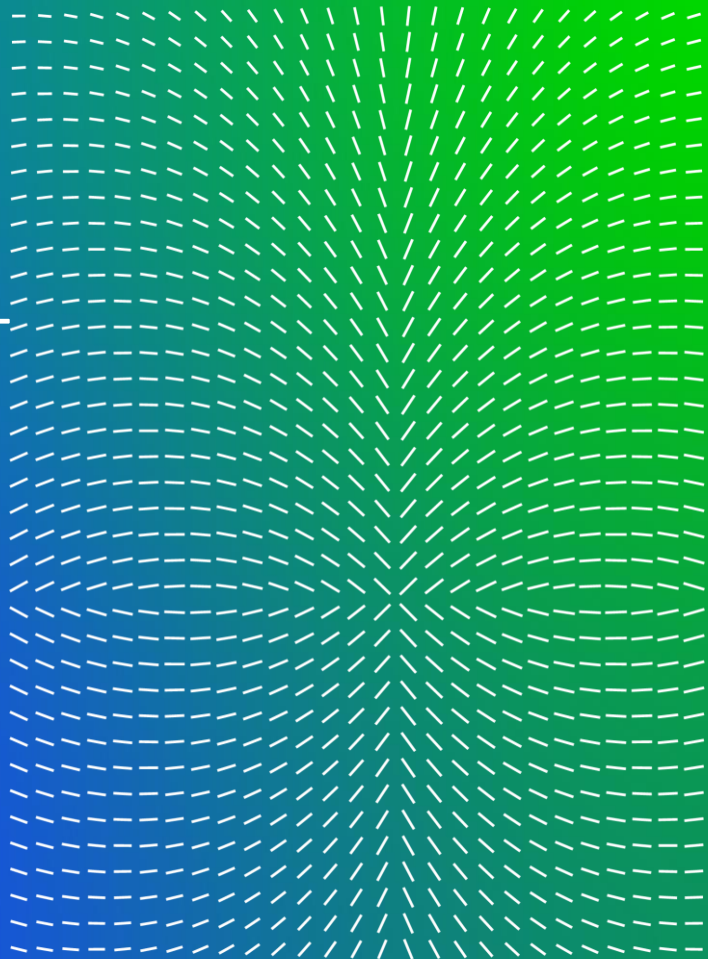


# Trellix

트렐릭스 보안 플랫폼,  
진화하는 위협에 대한 근본적 대응

김 현섭 기술총괄

Trellix Korea



# Trellix Platform



XConsole



Endpoint Security



Data Security



Cloud Security



Email Security



Network Security



3<sup>rd</sup> Party Engine

Core  
Engines



Advanced  
Research  
Center



Product Research



Threat Intelligence



Adversarial Resilience  
& Advocacy



Data Science ML / AI

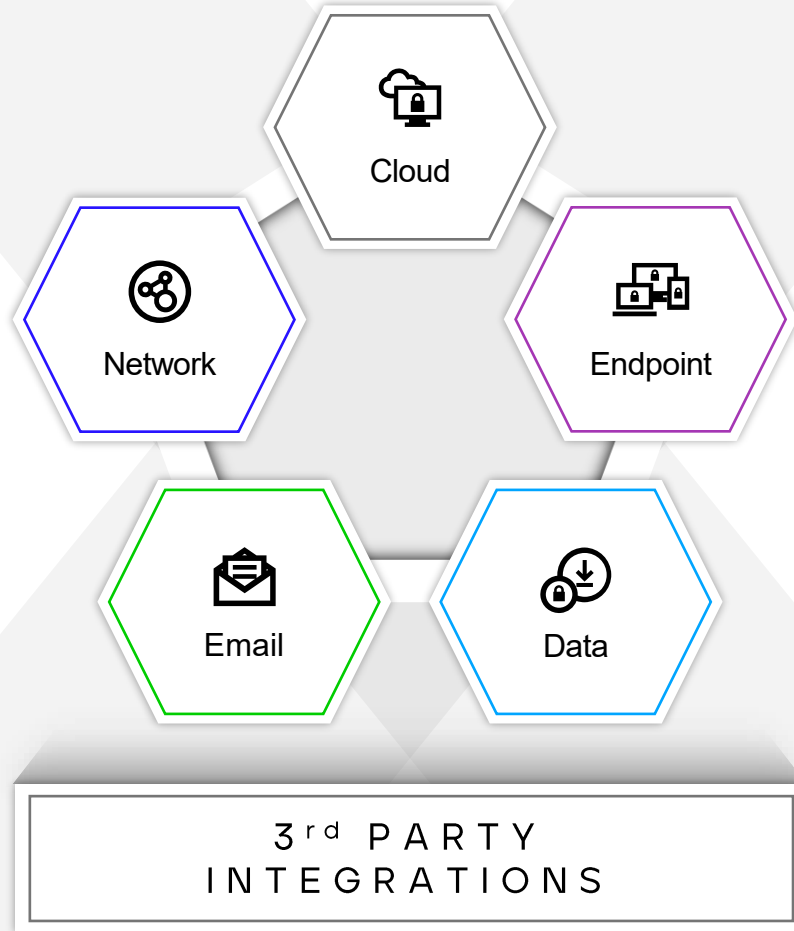


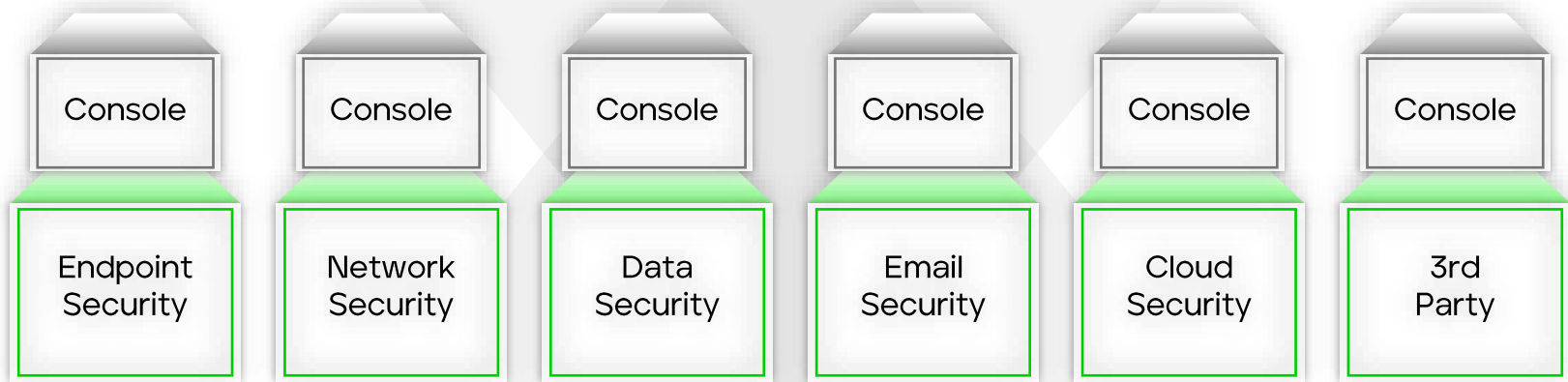
Research Engineering

Data Lake



# Trellix Product Lines





**XConsole**

UX + APIs

Endpoint  
Security

Network  
Security

Data  
Security

Email  
Security

Cloud  
Security

3rd  
Party

**Core Engines**

NEW

# XConsole

**McAfee™**  
EDR  
(EDR)

**Trellix**  
Unified  
Endpoint

**FIREEYE™**  
HX  
(EDR + Forensics)

## OUTPUT

Endpoint Protection Platform
Endpoint Detection & Response
Forensics
Windows, Mac, Linux

# Trellix Endpoint Security

Trellix Endpoint Security (ENS)



Malware Protection

Trellix Application and Change Control



Deny/Allow Lists

Trellix Device Control



USB Device Blocking

Trellix EDR



Threat Mitigation

Trellix Forensics (HX)



Endpoint Forensics

Trellix Policy Auditor



Compliance

Trellix Cloudvisory



Cloud Security Posture Management

Trellix Desktop Encryption



Protecting the device

Trellix Host Data Loss Prevention



Protecting the Data

Trellix Mobile Security



Protecting the mobile device

# Trellix Unified Security

e Policy Orchestration



Trellix Agent (TA)



BETA : Q4

Endpoint

Trellix Endpoint Security (ENS)



Malware Protection

Trellix Application and Change Control



Deny/Allow Lists

Trellix Device Control



USB Device Blocking

Trellix EDR



Threat Mitigation

Trellix Forensics (HX)



Endpoint Forensics

Trellix Policy Auditor



Compliance

Trellix Cloudvisory



Cloud Security Posture Management

Trellix Desktop Encryption



Protecting the device

Trellix Host Data Loss Prevention



Protecting the Data

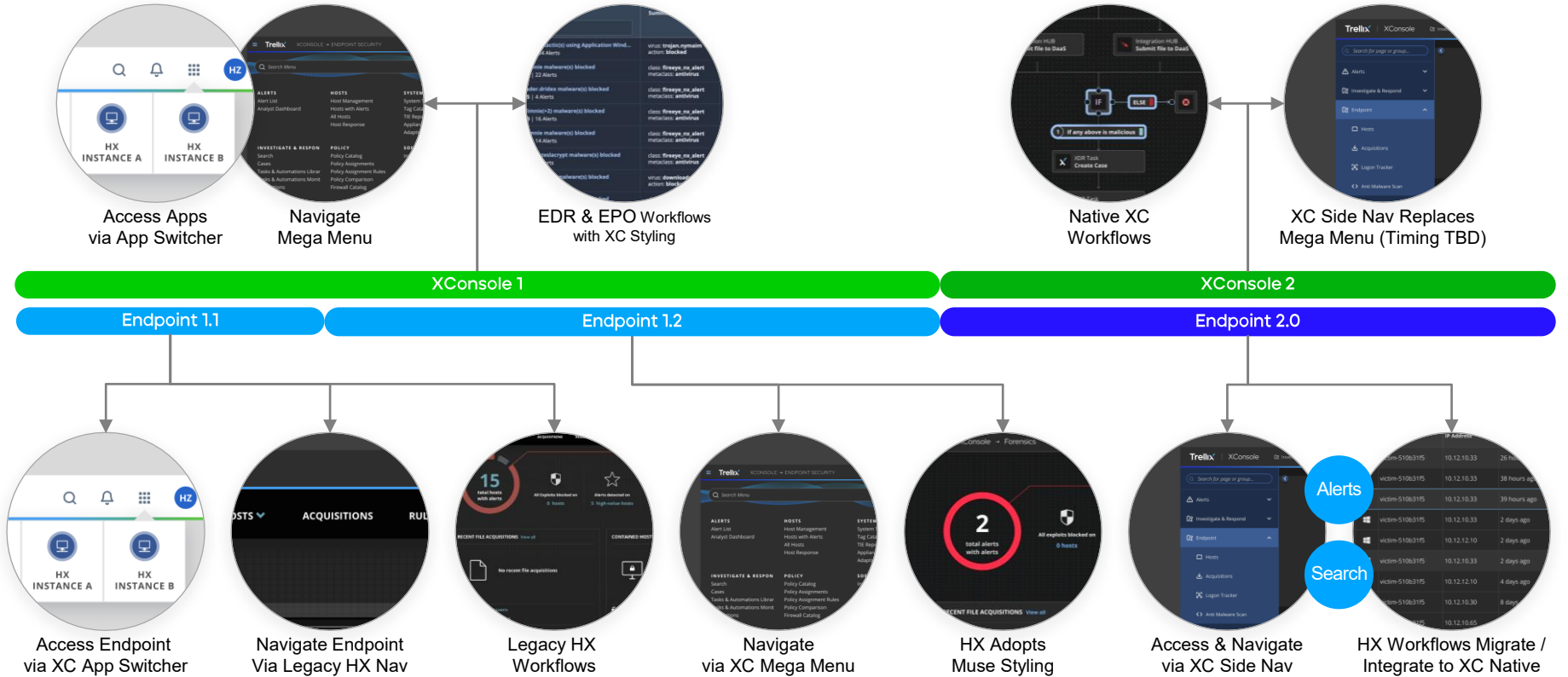
Trellix Mobile Security



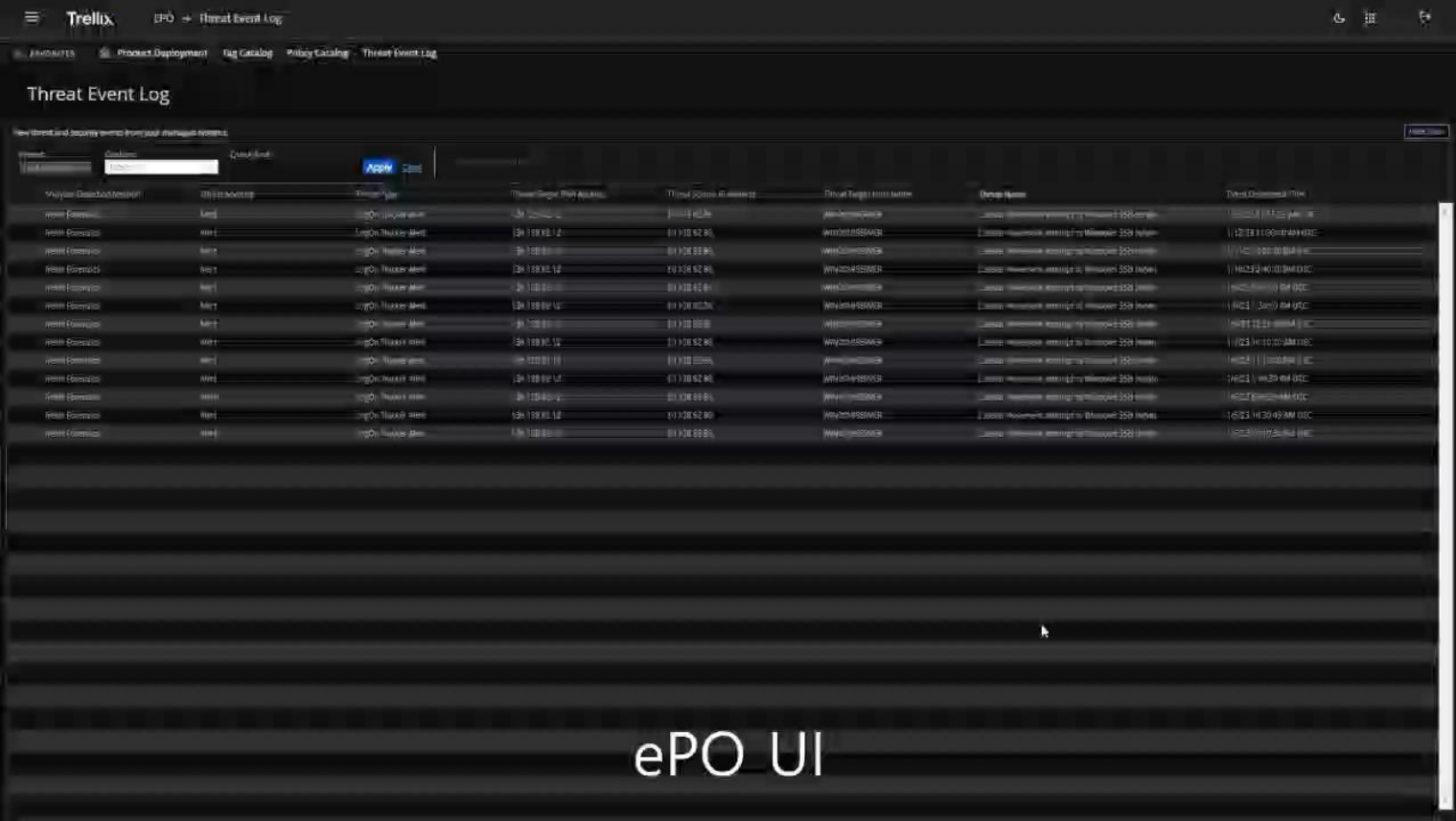
Protecting the mobile device



# XConsole / Endpoint 단계별 연동



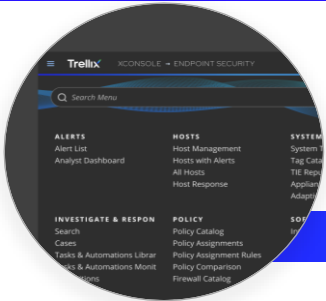
# Trellix Unified Endpoint Security Experience



ePO UI

# Trellix Network / Email Security





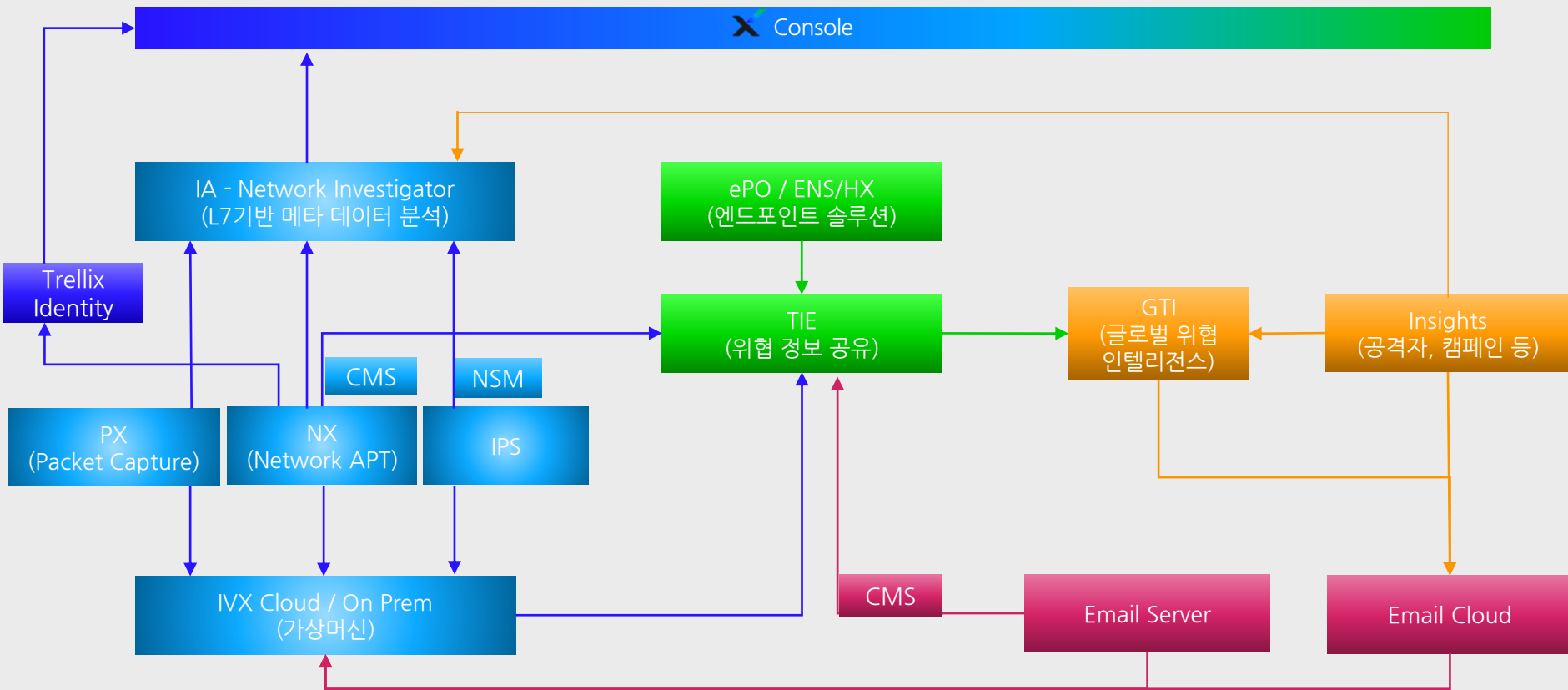
Console



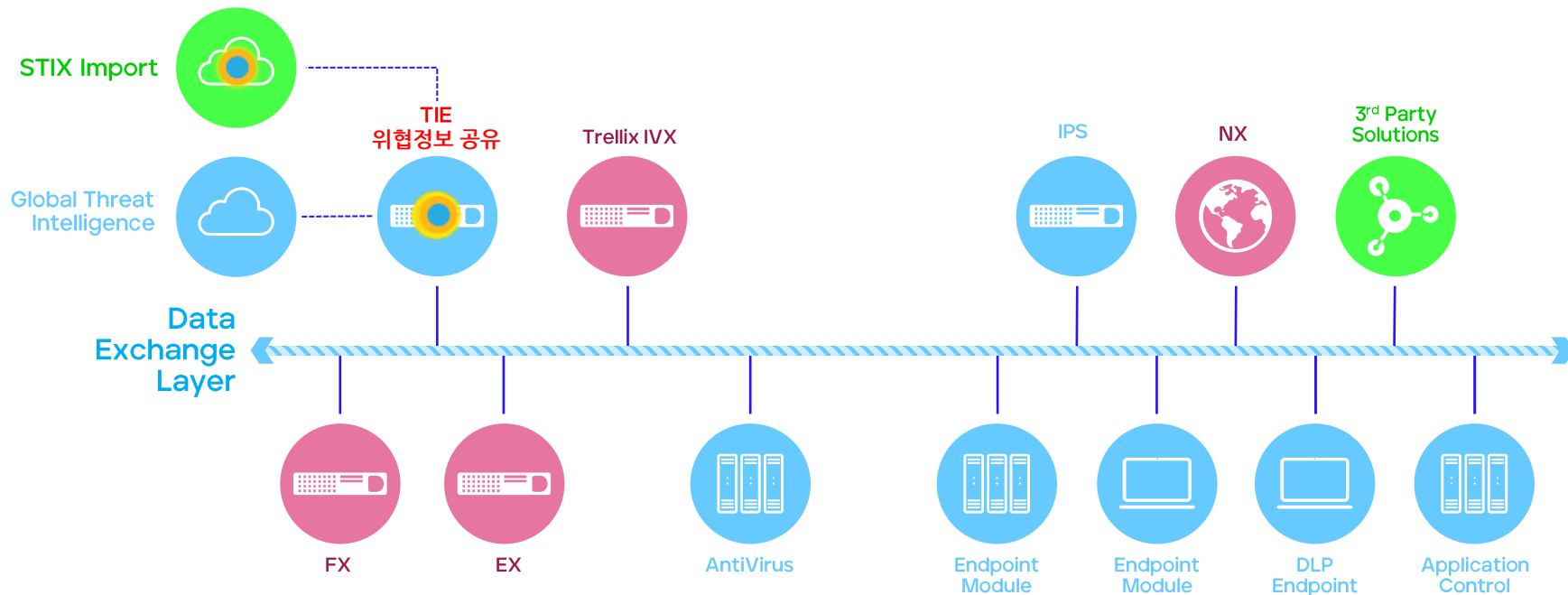
Trellix

# NEBU Portfolio

포트폴리오 전반에 걸쳐 통합



# 기업 내에 위협 정보 교환 모델 (TIE)



**XConsole**

UX + APIs

Endpoint  
Security

Network  
Security

Data  
Security

Email  
Security

Cloud  
Security

3rd  
Party

**Core Engines**

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



# Open & Native

TRELLIX Products portfolio

IT/SecOps    Researcher    Partner    MSSP

**XConsole**  
UX + APIs

**Trellix XDR Platform**  
Correlation + Contextualization + Playbooks

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

**Trellix** ADVANCED RESEARCH CENTER  
• Knowledge services

**DATA LAKE**

TRELLIX EVENT FABRIC (API)

## Core Engines

Endpoint Security	Network Security	Data Security	Email Security	Cloud Security	3rd Parties												
<ul style="list-style-type: none"> <li>• End Point Security</li> <li>• EDR</li> <li>• Forensic</li> </ul> <p>Trellix Unified EndPoint Security Platform</p>	<ul style="list-style-type: none"> <li>• Network Security (NX)</li> <li>• Network IPS (NSP)</li> <li>• Network Forensic (PX)</li> <li>• Sandbox (IVX)</li> </ul> <p>Trellix Network Investigator (NDR)</p>	<ul style="list-style-type: none"> <li>• Device Control</li> <li>• Encryptions</li> <li>• Enterprise DLP (eDLP, nDLP, Gateway DLP, Cloud DLP)</li> </ul> <p>Trellix ENT DLP Solution</p>	<ul style="list-style-type: none"> <li>• Advanced Email Security / APT (On-Premise &amp; Cloud)</li> <li>• Sandbox (IVX)</li> </ul> <p>Collaboration Security</p>	<ul style="list-style-type: none"> <li>• Sandbox (IVX &amp; DaaS)</li> <li>• Skyhigh Security</li> <li>• SIEM/HELIX/ePO</li> </ul> <p>Security Operations</p>	<p>100+ Vendors 200+ Plug-ins</p> <p>650+ Parsers 75+ Cloud Connectors</p> <table border="1"> <tr><td>Atlassian Jira</td><td>AWS GuardDuty</td></tr> <tr><td>CB Endpoint</td><td>Cisco Umbrella</td></tr> <tr><td>IBM Qradar</td><td>Netskope</td></tr> <tr><td>Okta</td><td>Palo Alto Prisma</td></tr> <tr><td>ThreatQ</td><td>ServiceNow</td></tr> <tr><td>Symc Bluecoat</td><td>Windows Defenc</td></tr> </table>	Atlassian Jira	AWS GuardDuty	CB Endpoint	Cisco Umbrella	IBM Qradar	Netskope	Okta	Palo Alto Prisma	ThreatQ	ServiceNow	Symc Bluecoat	Windows Defenc
Atlassian Jira	AWS GuardDuty																
CB Endpoint	Cisco Umbrella																
IBM Qradar	Netskope																
Okta	Palo Alto Prisma																
ThreatQ	ServiceNow																
Symc Bluecoat	Windows Defenc																

TRELLIX Products portfolio

# 탐지/분석 대상의 확대

통합 보안 운영 프로세스 제공 (보안 운영 플랫폼)



로그 수집



자동화



실시간 탐지



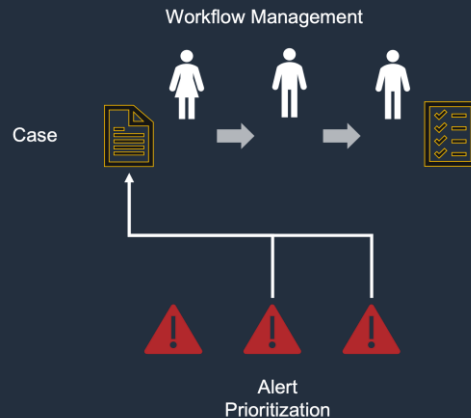
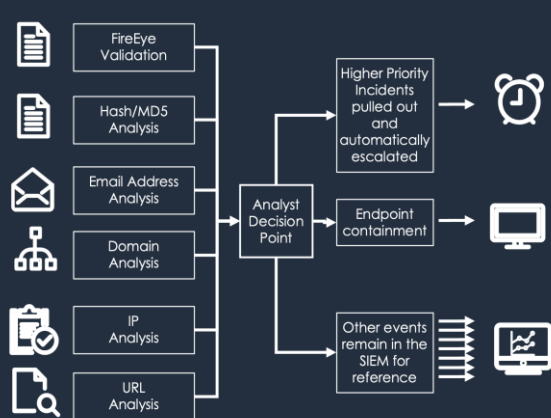
우선순위



분석/조사



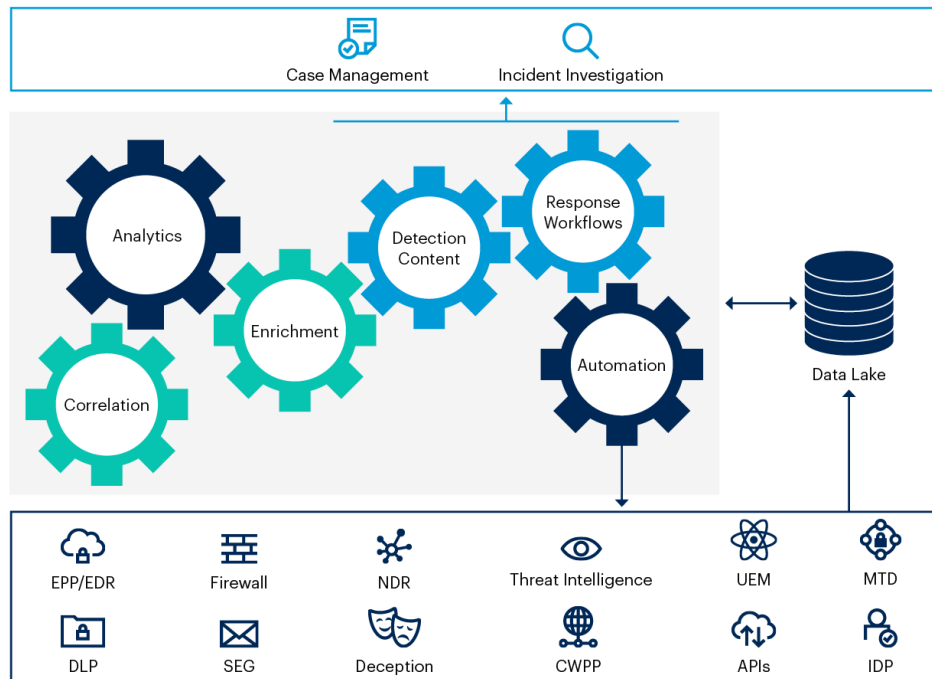
대응/조치



# 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

## XDR이 제공하는 전반적인 효과

- 다양한 센서로부터 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

The screenshot displays the Trellix Threats dashboard. At the top, it says "Welcome to your Dashboard, TonyKim" and "There are 5,876 threats. 2 of them must be reviewed as soon as possible and 76 recommended to be reviewed proactively." Below this is a list of "Top 6 Threats". The first threat is highlighted with a red box. It has an ID of 826 and was detected on 2023-09-11T13:25:39.093783Z. The description is "Collection(+9) tactic(s) using Brute Force(+22) technique(s) with generic.shellcode.ode.marte.c.e6ab95e0(+15) malware(s) detected,...". The status is "Open" and it is currently "Unassigned". To the right of the list is a "Total Risk Score" chart showing a line graph with a peak at 15,000 on 09-11 and a current score of 883 on 09-17. Below the chart is a section for "Assigned Threats" which currently shows "No data to display".

**Threats Overview**

Welcome to your Dashboard, TonyKim

There are **5,876** threats. **2** of them must be reviewed as soon as possible and **76** recommended to be reviewed proactively. [Learn More](#)

Threats: All | Status: Open | Assignee: All | Tags: All | Show: Past 7 Days

Top 6 Threats | View All 526 Threats

ID	Description	Status	Assignee	Actions
826	CORRELATIONS   ID: 85782   DETECTED AT: 2023-09-11T13:25:39.093783Z Collection(+9) tactic(s) using Brute Force(+22) technique(s) with generic.shellcode.ode.marte.c.e6ab95e0(+15) malware(s) detected,... Collection(+9) tactic(s) using Brute Force(+22) technique(s) with generic.shellcode.ode.marte.c.e6ab95e0(+15) malware(s) detected, but not blocked on system(+3)...	Open	Unassigned	Open, Assign, Share, +1
790	CORRELATIONS   ID: 87674   DETECTED AT: 2023-09-15T10:00:00.000000Z Command and Control(+6) tactic(s) using DNS(+14) techni...	Open	Unassigned	Assign, Share
700	CORRELATIONS   ID: 86784   DETECTED AT: 2023-09-11T12:00:00.000000Z Command and Control(+7) tactic(s) using Bypass User Acc...	Open	Unassigned	Assign, Share
358	CORRELATIONS   ID: 86845   DETECTED AT: 2023-09-11T19:00:00.000000Z Collection(+6) tactic(s) using Automated Collection(+26) te...	Open	Unassigned	Assign, Share
356	CORRELATIONS   ID: 87148   DETECTED AT: 2023-09-12T12:00:00.000000Z Collection(+6) tactic(s) using Accessibility Features(+14) te...	Open	Unassigned	Assign, Share
356	CORRELATIONS   ID: 87628   DETECTED AT: 2023-09-14T20:00:00.000000Z Collection(+8) tactic(s) using Credential API Hooking(+26) t...	Open	Unassigned	Assign, Share

Total Risk Score | Show: Past 7 Days

RISK SCORE: 883

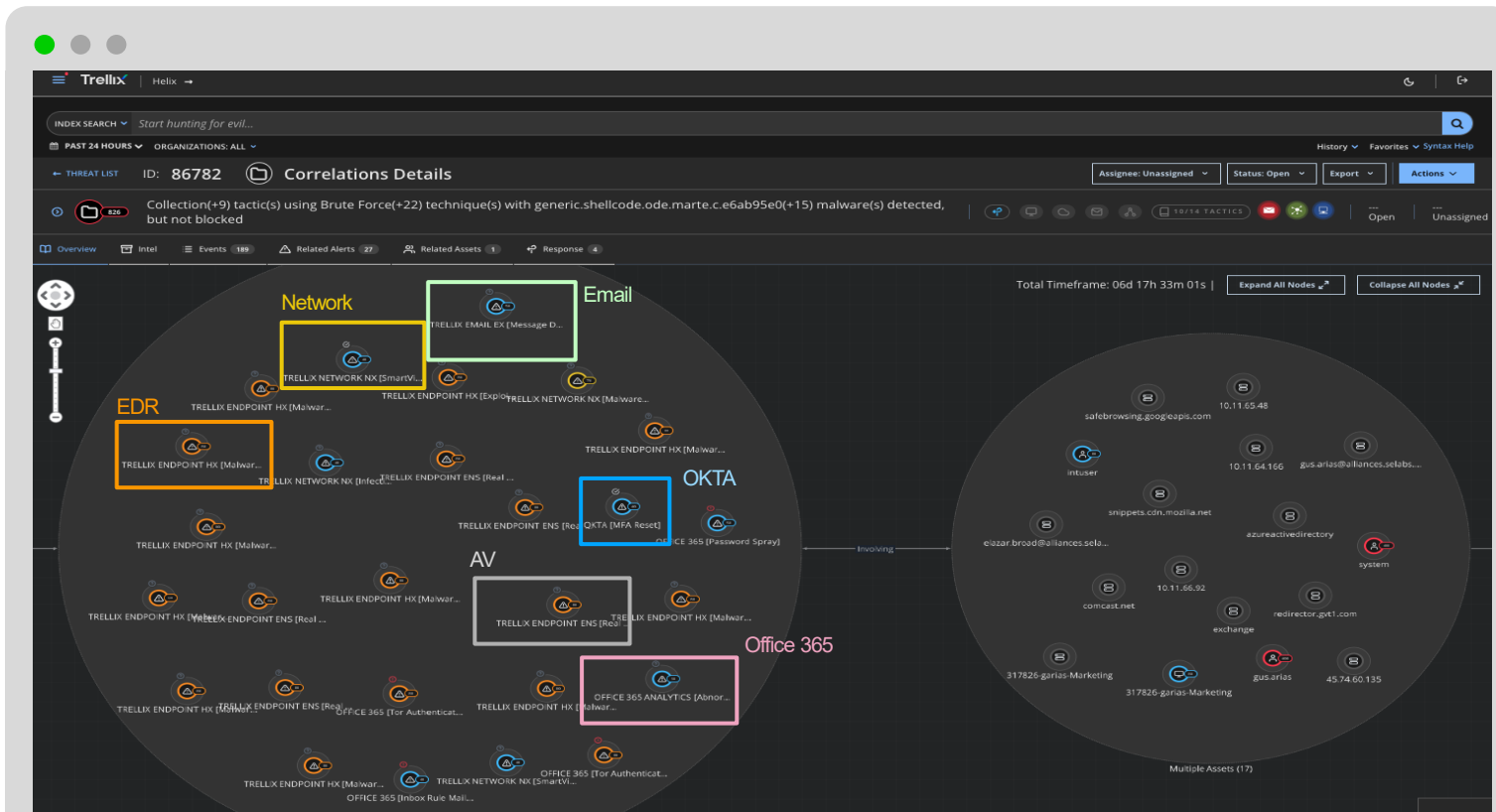
Assigned Threats | Show: Past 7 Days

No data to display

# 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

The screenshot shows the Trellix Helix Threats interface. The main header displays 'Trellix Helix -> Threats' and 'Correlations Details' for threat ID 86782. The threat is categorized as 'CRITICAL' and 'Unassigned'. The description reads: 'Collection(+9) tactic(s) using Brute Force(+22) technique(s) with generic.shellcode.ode.marte.c.e6ab95e0(+15) malware(s) detected, but not blocked'. Below this, a 'Playbook Activity' flowchart is visible, showing steps like 'Update Case', 'Extract Hashes', and 'Check Hashes'. A red box highlights the 'Trellix Intelligent Virtual Execution (IVX): Hashes Enrichment' step in the flowchart. To the right, a detailed view of this step is shown, including a search bar, a list of activities, and input/output details.

**Trellix Intelligent Virtual Execution (IVX): Hashes Enrichment**

Copy Playbook Activity Download Activity Expand All Collapse All

element\_labels.manual\_trigger 2023-09-12 20:45 UTC

Update Case 2023-09-12 20:45 UTC

Extract Hashes 2023-09-12 20:45 UTC

**INPUT (\$)**

Threat type	correlation_group
Threat id	86782
Mid 5 hashes	["a01ff21d954f5be16438cc6c7530bbe8"; "844fa888c909313837dc1dbccd0d591"; "57f494..."]
Hex id	hexcc0656
Alert json	

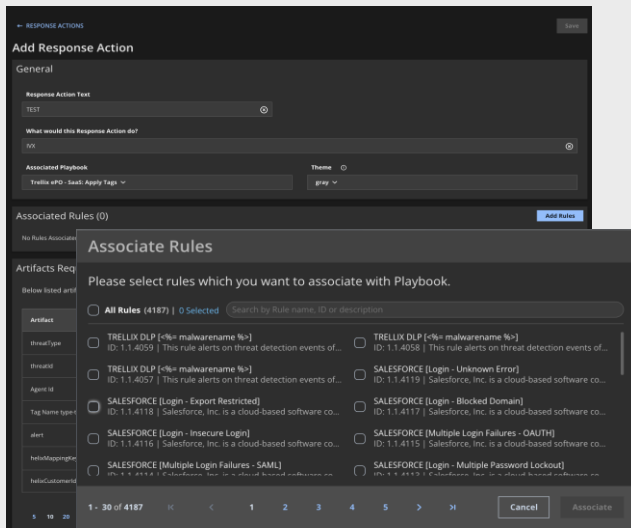
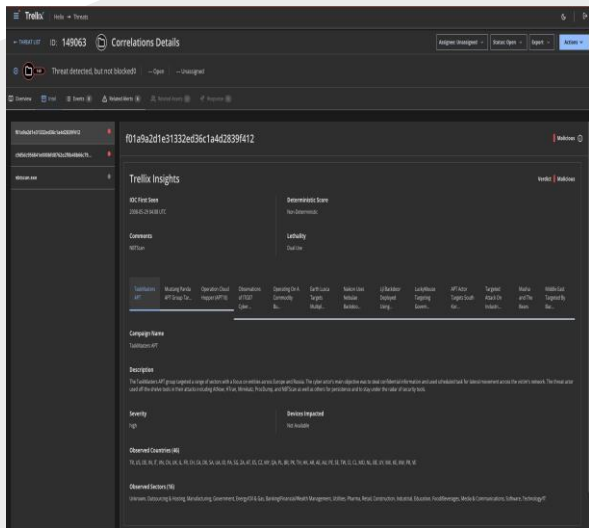
**OUTPUT (\$)**

Threat type	correlation_group
Success	true
Hex id	hexcc0656
Hashes	["a01ff21d954f5be16438cc6c7530bbe8"; "844fa888c909313837dc1dbccd0d591"; "57f494..."]

# 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**