Trellix

Cyber Resilience

The evolution of cybersecurity

Ron Wang
Gustavo Arias

July 9, 2024

Speaker Intro

Ron Wang

Senior Director,
APJ Solutions Engineering

Gustavo Arias

Principal Solutions Engineer,
Trellix

Agenda

1. The World we live in.
2. The problem we are trying to solve
3. Trellix Investment
4. Platform Approach

Trellix

The world we live in……

Global Threat Landscape

Data Breaches

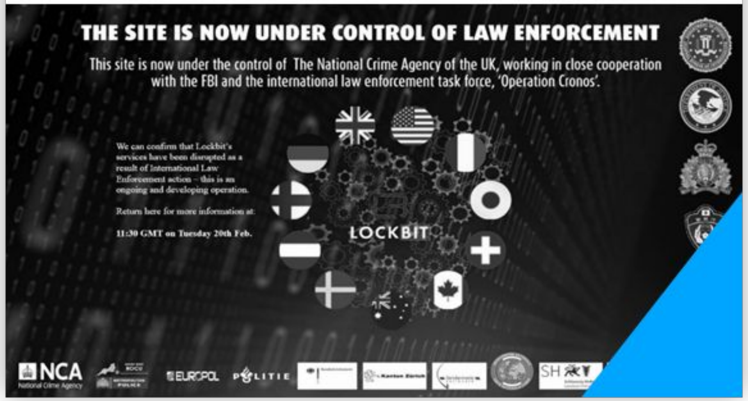
The alleged leakage of classified documents and sensitive data raises concerns regarding national security, privacy, and the integrity of critical information.

Geopolitical Tensions

Governments faces diverse cyber threats, including state-sponsored attacks on critical infrastructure, cyber espionage targeting sensitive data, and disruptive actions by nation-states actors.

Ransomware

Reports show that many countries are increasingly confronted with ransomware attacks, posing significant challenges to critical infrastructure, government agencies, and businesses.



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

A changing landscape:

Cyber Industry Disruptions

- AI Imperative
- Business Automation Security
- SecOps workflow efficiency: Investigation & Response
- Risk and Liability

Trellix

The problem we are trying to solve

Today’s SOC Challenges

Siloed tools that don't work together

Fragmented visibility and control

Limited org resources and expertise

Overworked teams and insufficient threat coverage

Too many alerts and missed threats

Alert fatigue and high-risk exposure

Expensive infrastructure

Costly to maintain and operate

SOCs struggle to keep up with threat landscape of multi-vector attacks= Risk

Trellix

Trellix Zero Trust Strategy

Methodology

What is Zero Trust?

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

https://csrc.nist.gov/publications/detail/sp/800-207/final

Trellix

Our Approach to DOD Zero Trust

1

Data is your most important asset

Mission resiliency is critical

2

XDR is a core requirement of ZT under the Device pillar

3

Embrace a multi-vendor approach through an open platform

4

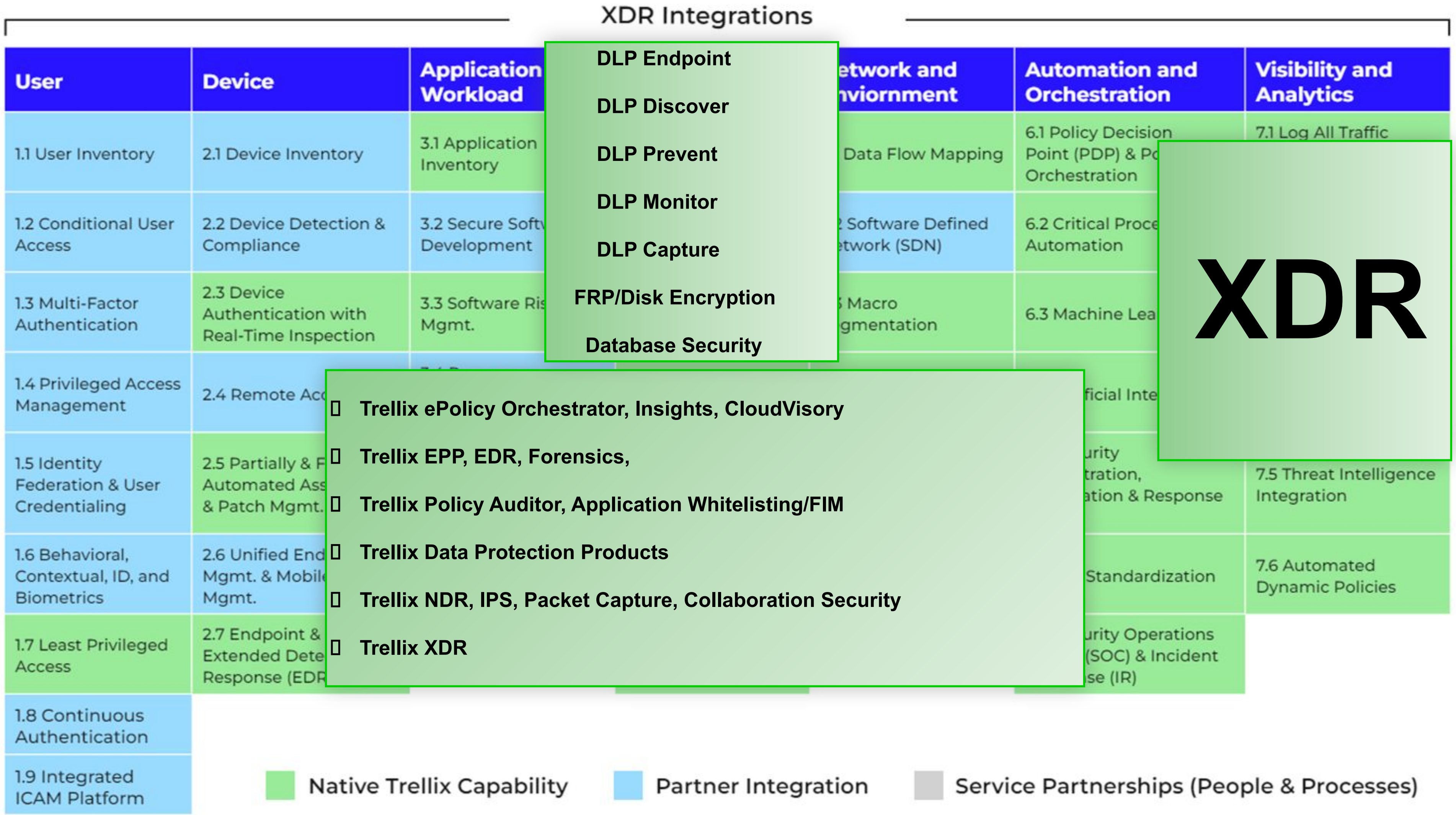
Prioritize and automate SecOps workflows across all controls

5

Aggressive development and partnership to meet ZT requirements

Trellix

XDR aligns the DoD’s 7 Pillars of Zero Trust



XDR Integrations

User	Device	Application Workload		etwork and nviornment	Automation and Orchestration	Visibility and Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory		Data Flow Mapping	6.1 Policy Decision Point (PDP) & Po Orchestration	7.1 Log All Traffic
1.2 Conditional User Access	2.2 Device Detection & Compliance	3.2 Secure Softv Development		2 Software Defined twork (SDN)	6.2 Critical Proce Automation	
1.3 Multi-Factor Authentication	2.3 Device Authentication with Real-Time Inspection	3.3 Software Ris Mgmt.		3 Macro gmentation	6.3 Machine Lea	
1.4 Privileged Access Management	2.4 Remote Acc				ficial Inte	
1.5 Identity Federation & User Credentialing	2.5 Partially & F Automated Ass & Patch Mgmt.				urity tration, ation & Response	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual, ID, and Biometrics	2.6 Unified End Mgmt. & Mobile Mgmt.				Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Dete Response (EDR				urity Operations (SOC) & Incident se (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

DLP Endpoint

DLP Discover

DLP Prevent

DLP Monitor

DLP Capture

FRP/Disk Encryption

Database Security

XDR

- Trellix ePolicy Orchestrator, Insights, CloudVisory
- Trellix EPP, EDR, Forensics,
- Trellix Policy Auditor, Application Whitelisting/FIM
- Trellix Data Protection Products
- Trellix NDR, IPS, Packet Capture, Collaboration Security
- Trellix XDR

🟩 Native Trellix Capability 🟦 Partner Integration ⬜ Service Partnerships (People & Processes)

Trellix

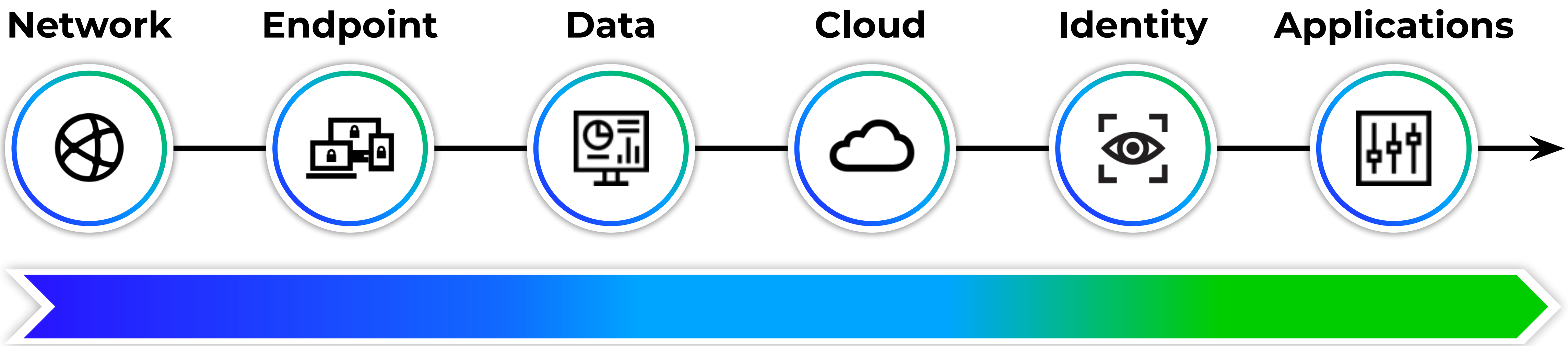
XDR is Essential to a Zero Trust Strategy

PREVENTION
DETECTION
Users
Devices
Data
Environments

Trellix

Zero Trust & XDR:

Inspired by the Same Business Problem



XDR: Detect & Remediate Faster, Cheaper

Faster Responses

Leverage Investments

Reduce Risk

Orchestration & Automation

XDR in Action

Social Engineering	First-factor Credential	MFA Fatigue	Lateral Movement	Data Exfiltration
With XDR:	Prioritized, Multi-vector detection	Lockdown, containment, rollback	Investigate, remediate in hours	Proactively address risk

Trellix

to add video.. play with click

XDR is Essential to a Zero Trust Strategy

Find the Unexpected

Increase Efficacy & Efficiency

Unlock Your Data

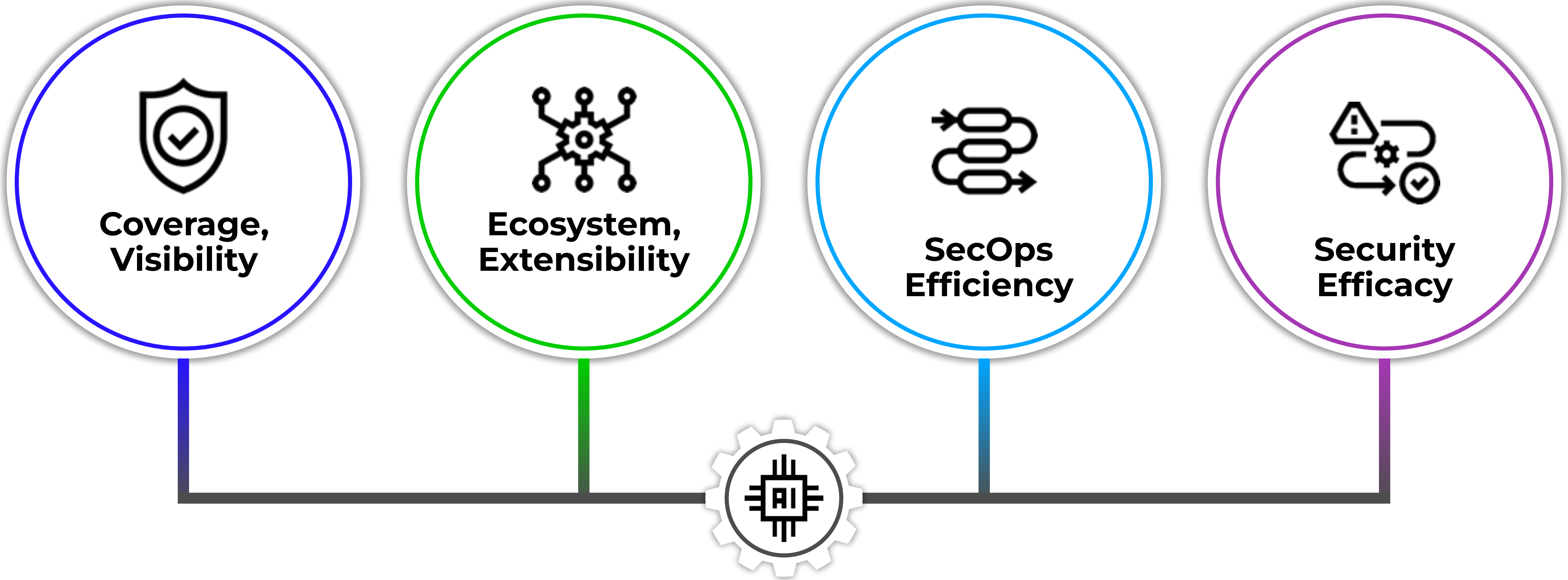
Trellix: The fastest path to XDR

Avg. deployment 7 days

Trellix Investment

We scale to protect our customers

Trellix Product Investment Areas



Coverage, Visibility

Ecosystem, Extensibility

SecOps Efficiency

Security Efficacy

Threat Intelligence, AI, Automation

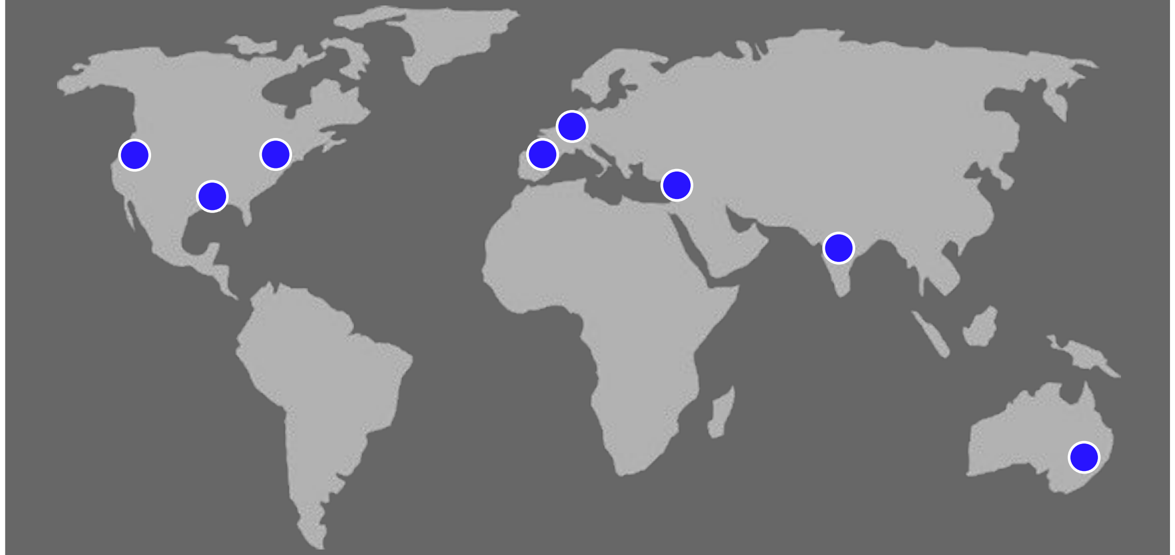
What This Means for You

- Preventing, detecting sophisticated attacks siloed tools miss
- Utilize current investments in your ecosystem
- Protecting critical data
- Upskilling teams, accelerating detection and response
- Lower operating costs

Threat Advance Research

Detection is our founding competency

Trellix Advanced Research



+200
researchers &
TI Analysts

+3600
Campaigns/2yrs

+100
Actors and tools with extensive tracking

+250
Different threat groups

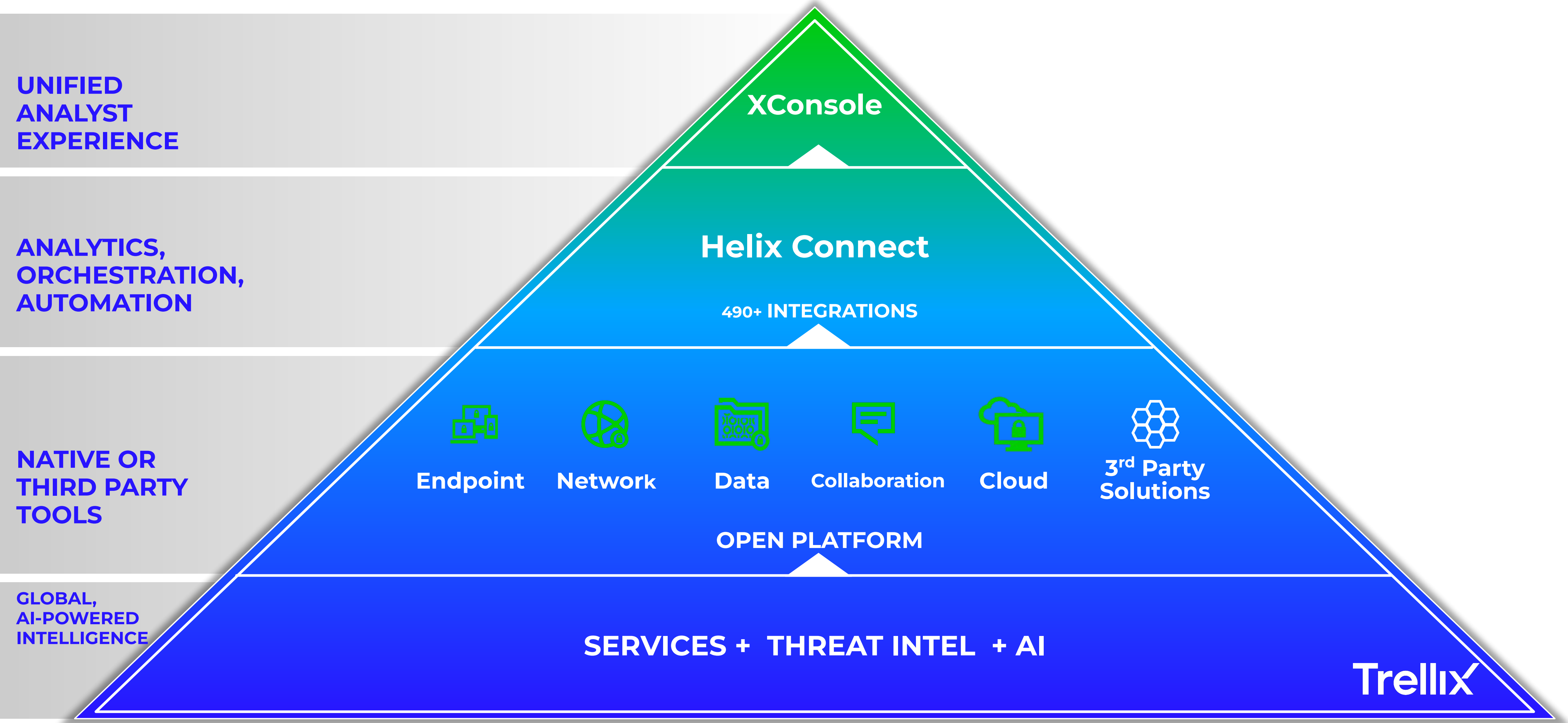
250M
Malicious file detections in last 30 days

+2250
Different malicious and non-malicious tools

1200
Unique customers/ 30 days with Campaign Detections

Trellix

The Trellix XDR Platform



UNIFIED ANALYST EXPERIENCE

XConsole

ANALYTICS, ORCHESTRATION, AUTOMATION

Helix Connect

490+ INTEGRATIONS

NATIVE OR THIRD PARTY TOOLS

Endpoint

Network

Data

Collaboration

Cloud

3rd Party Solutions

OPEN PLATFORM

GLOBAL, AI-POWERED INTELLIGENCE

SERVICES + THREAT INTEL + AI

Trellix