COMGUARD
communication security

Vize Trellix a plnohodnotné XDR

Martin Votava, Sales Director


Trellix


McAfee
FIREEYE
Trellix

Aby to nebylo moc jednoduché

Trellix

Skyhigh Security

Trellix

- Kompletní portfolio FireEye
  - Helix Security Platform
  - Network Security and Forensics
  - Email Security
  - Endpoint Security
  - …
- Portfolio McAfee
  - Endpoint security a EDR
  - Data Loss prevention and Encryption
  - IPS
  - SIEM
  - …

Skyhigh Security

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Access Network (ZTNA)
- Cloud Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI) technology
- Cloud Firewall
- Cloud Native Application Protection Platform (CNAPP)

What is XDR?

[XDR] s a platform that integrates, correlates and contextualizes data and alerts from multiple security prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple point solutions and advanced analytics to correlate alerts from multiple sources into incidents from weaker individual signals to create more accurate detections.

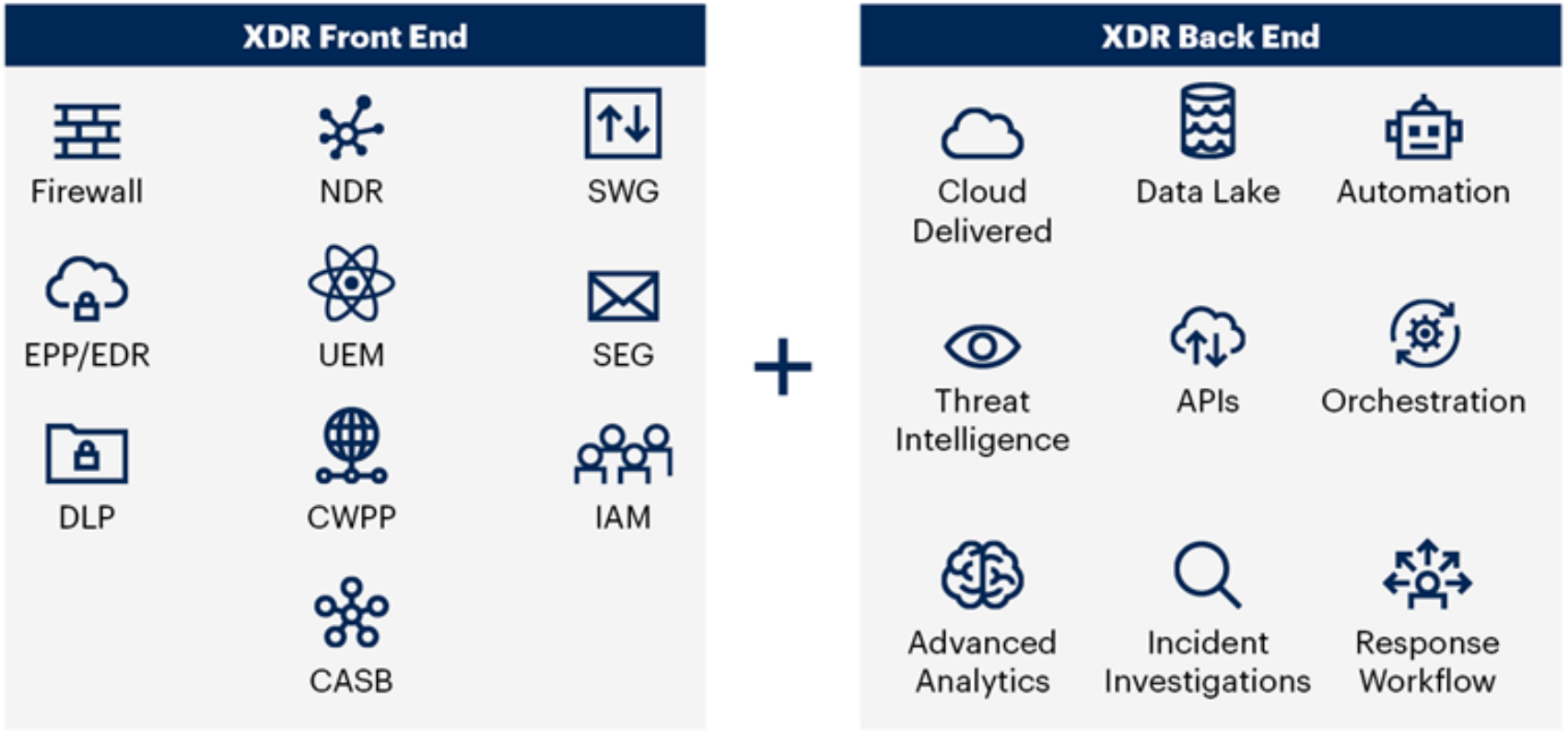
- Gartner, 2021 XDR Market Guide

Extended goes across several security vectors including endpoints, network, cloud, email and other third-party products.

Detection comes from the ability to detect and correlate threats across multiple vectors the moment they arise.

Response enables your organization to be better prepared to respond effectively to attacks in real time.

XDR Overview



Source: Gartner
747261_C

Gartner

Helix Platform

- Investigative Workflows
- SOAR and Threat Hunting Capability
- Event Streaming / Analytics

Detect on Demand

- Dynamic IOCs
- Analytics & ML
- File & URL Analysis
- Delivery & Payload
- Signatures

Threat Labs

- Contextual Threat Intelligence
- Automatic Enrichment and Correlation
- Mandiant + McAfee + NewCo

Workplace

- EPP/EDR/Forensics
- Data Protection
- Mobile Security
- Email Gateway
- Phishing Protection
- Business Email Compromise

Multi-Cloud

- Cloud Infrastructure Intrusion Prevention
- Data Center Intrusion Protection
- Server Protection
- Cloud Visibility
- Cloud Compliance
- Cloud Posture Assessment

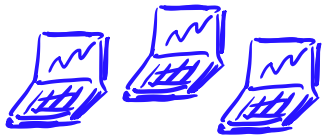
Partners (Not Exhaustive)

Phantom, splunk>, IBM QRadar, SWIMLANE, MANDIANT, MISP Threat Sharing, THREATQUOTIENT

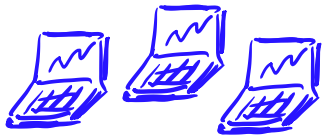
70+ Partners
650+ Parsers
150+ Plug-ins
75+ Cloud Connectors

aws, iboss, okta, Attivo Networks, Microsoft, TheHive, CYBERARK, ixia, slack

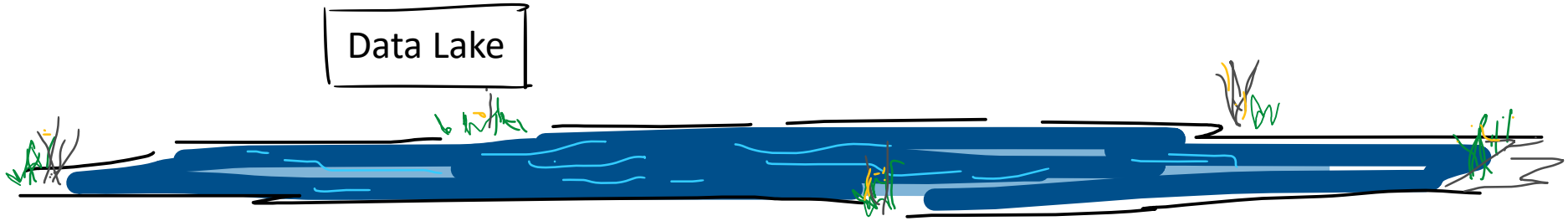
Why Trellix XDR



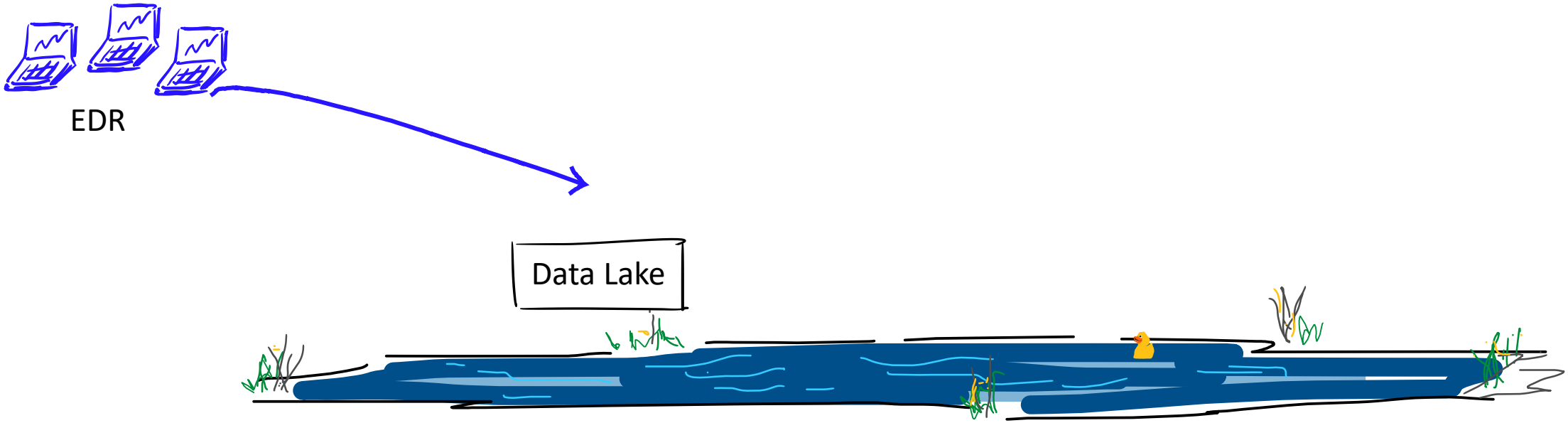
EDR

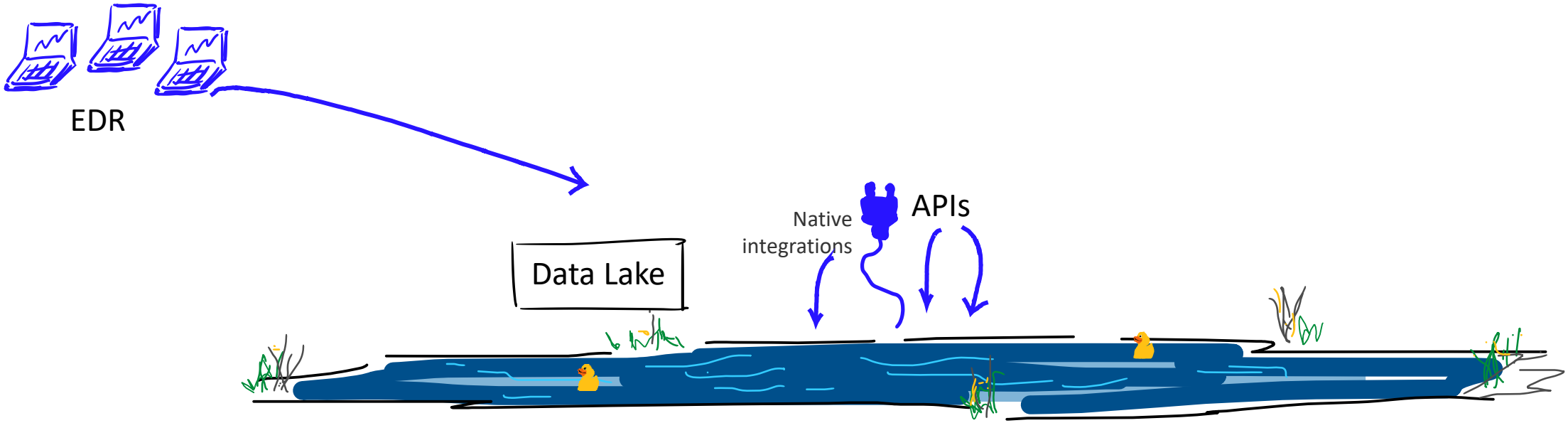


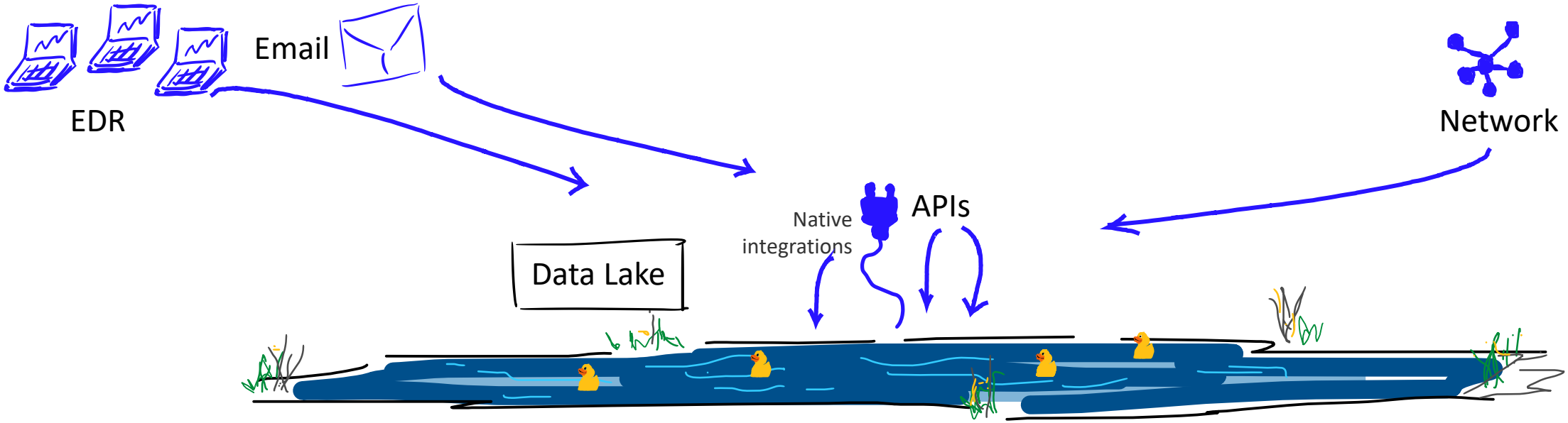
EDR

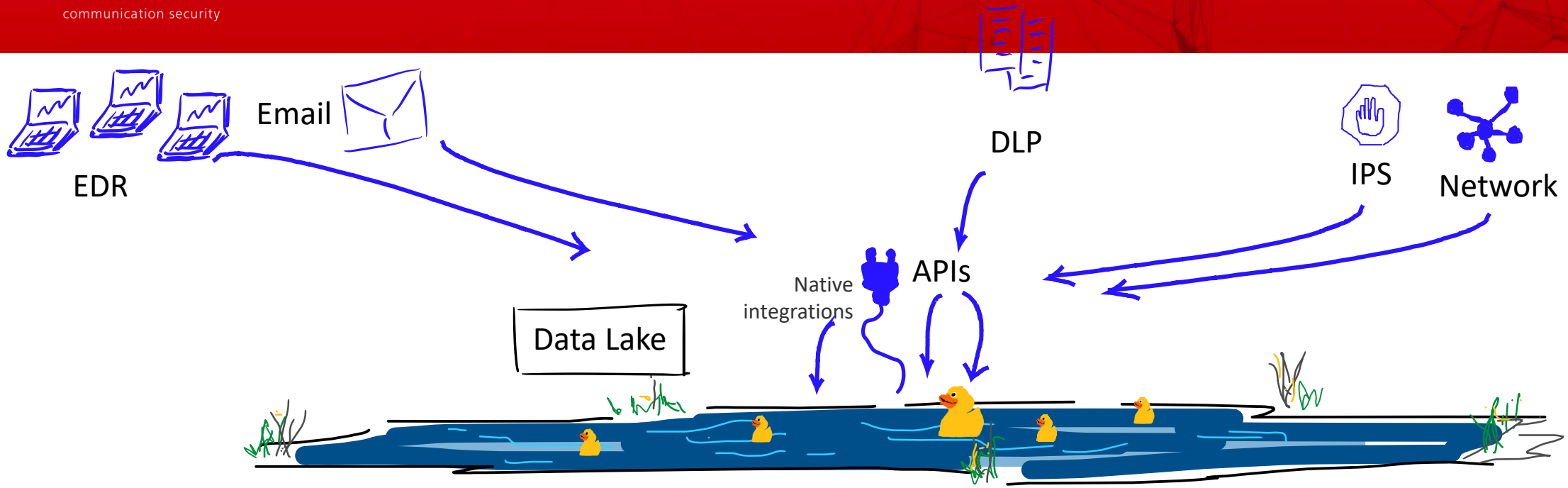


Trellix

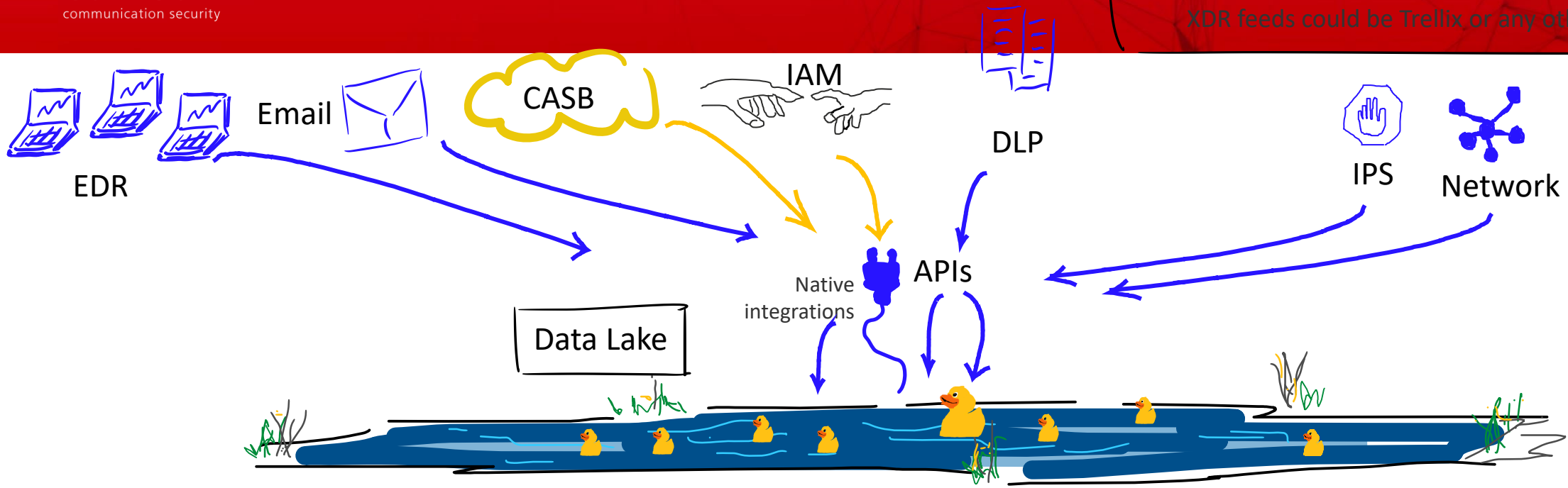

EDR
Data Lake


EDR
Data Lake
Native
integrations
APIs

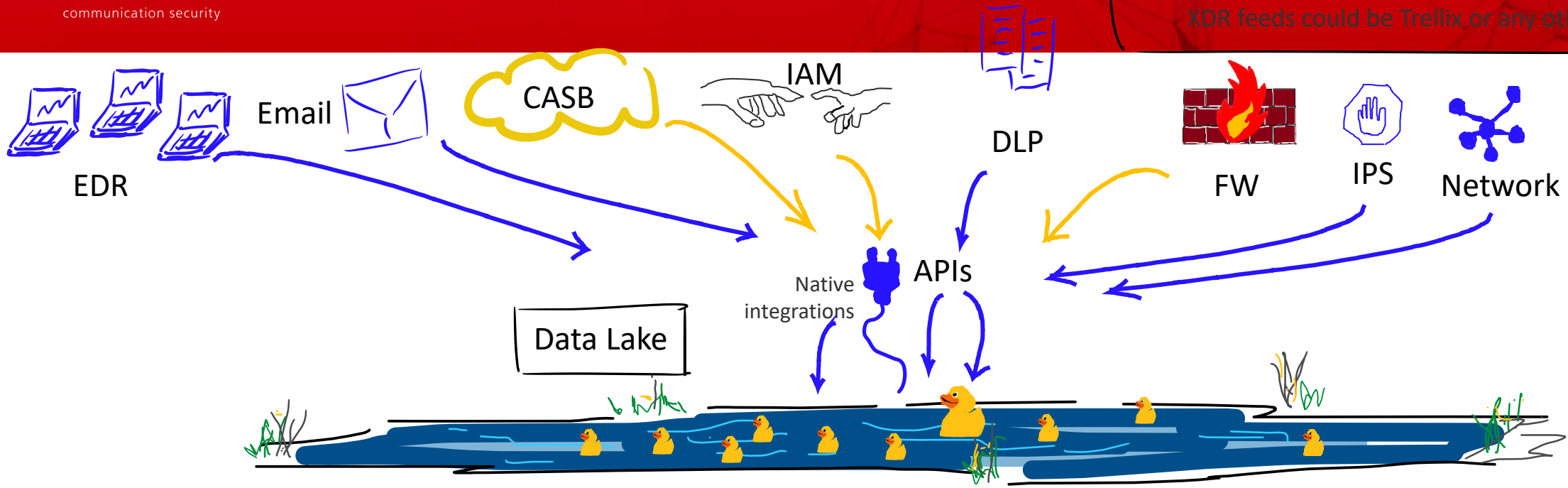

Email
EDR
Network
Native
integrations
APIs
Data Lake


Email
EDR
DLP
IPS
Network
APIs
Native
integrations
Data Lake

XDR feeds could be Trellix or any other vendor

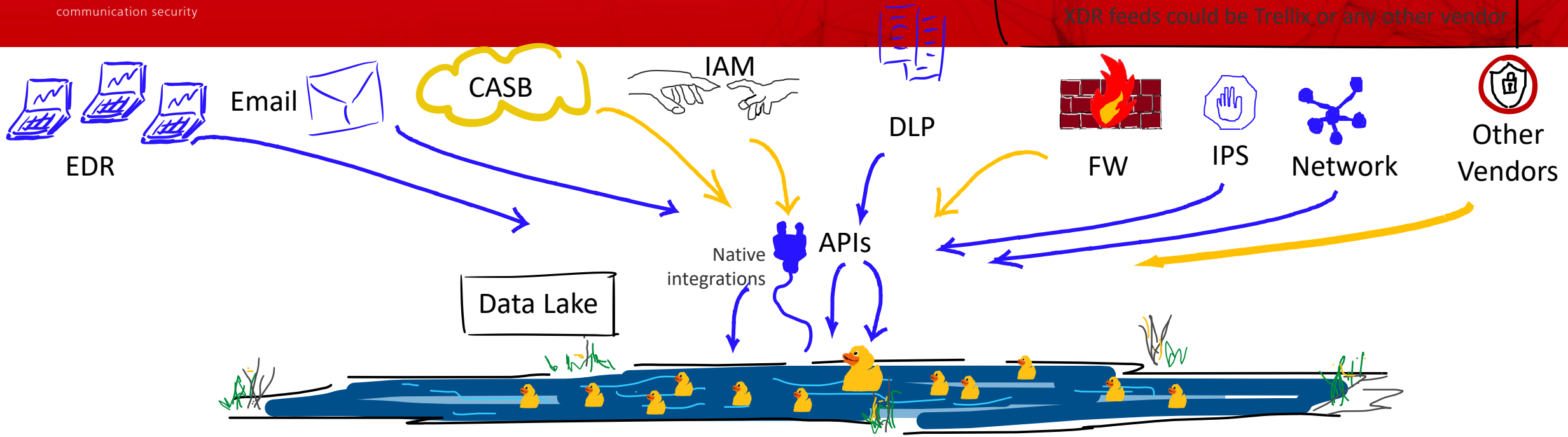


XDR feeds could be Trellix or any other vendor



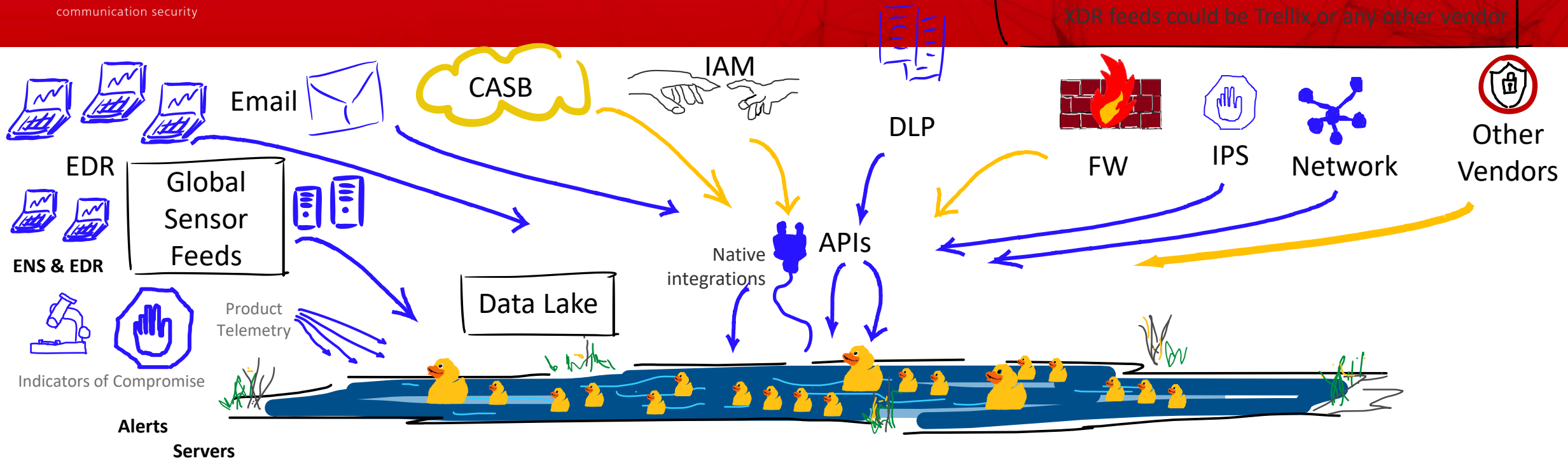
Trellix

XDR feeds could be Trellix or any other vendor



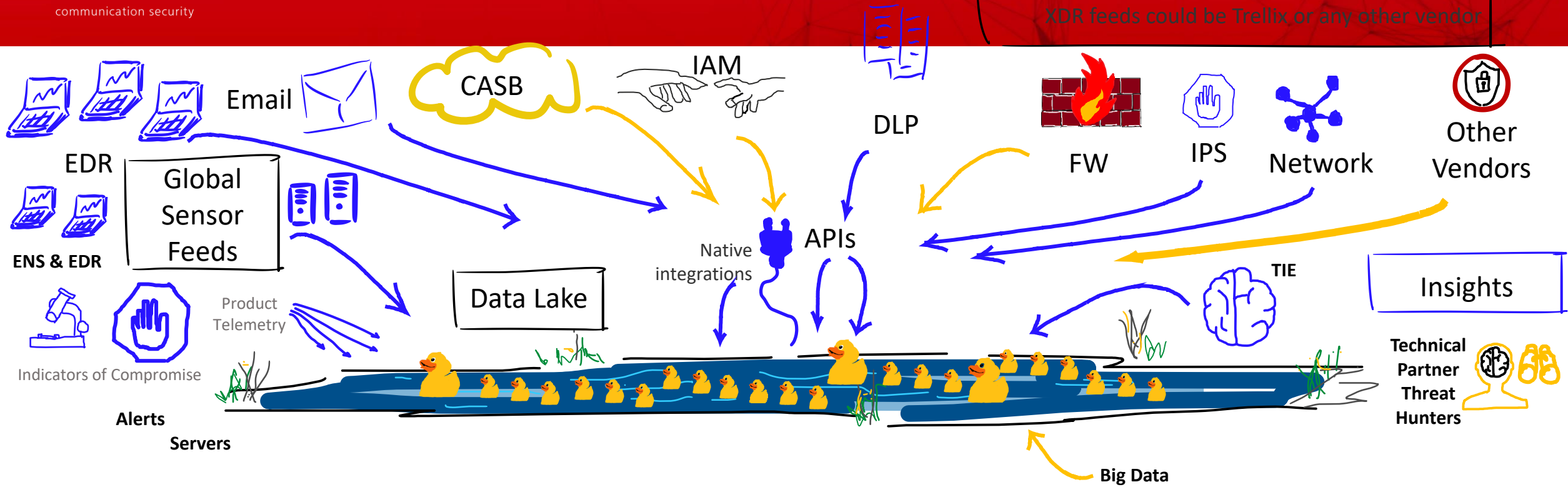
Trellix

XDR feeds could be Trellix or any other vendor



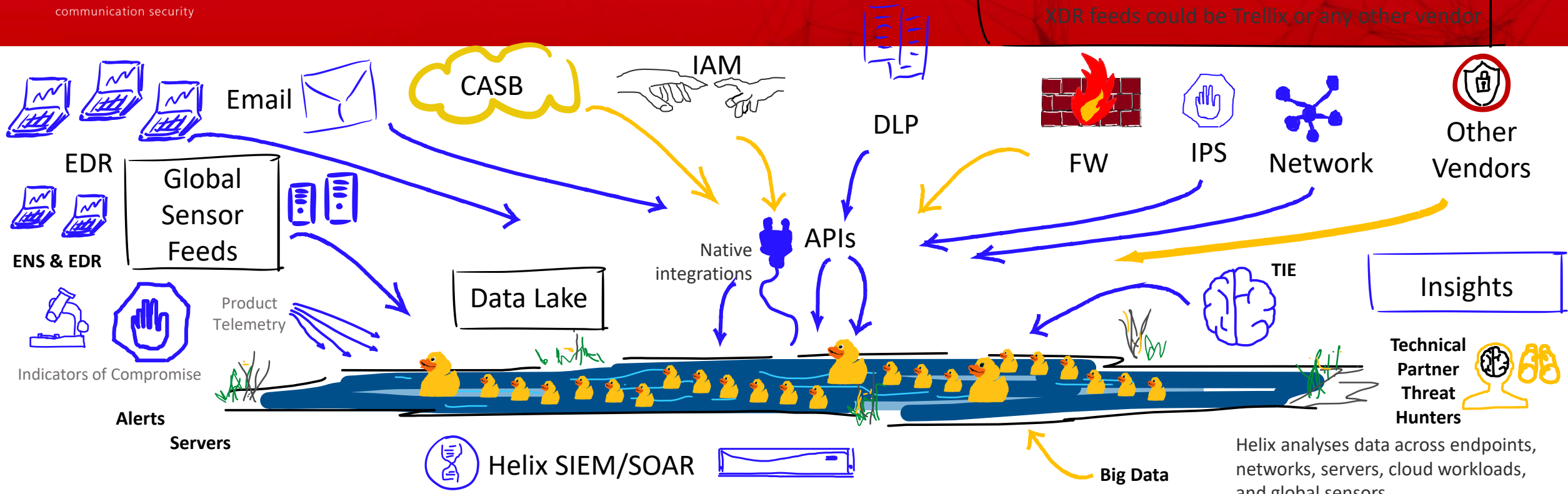
Trellix

XDR feeds could be Trellix or any other vendor



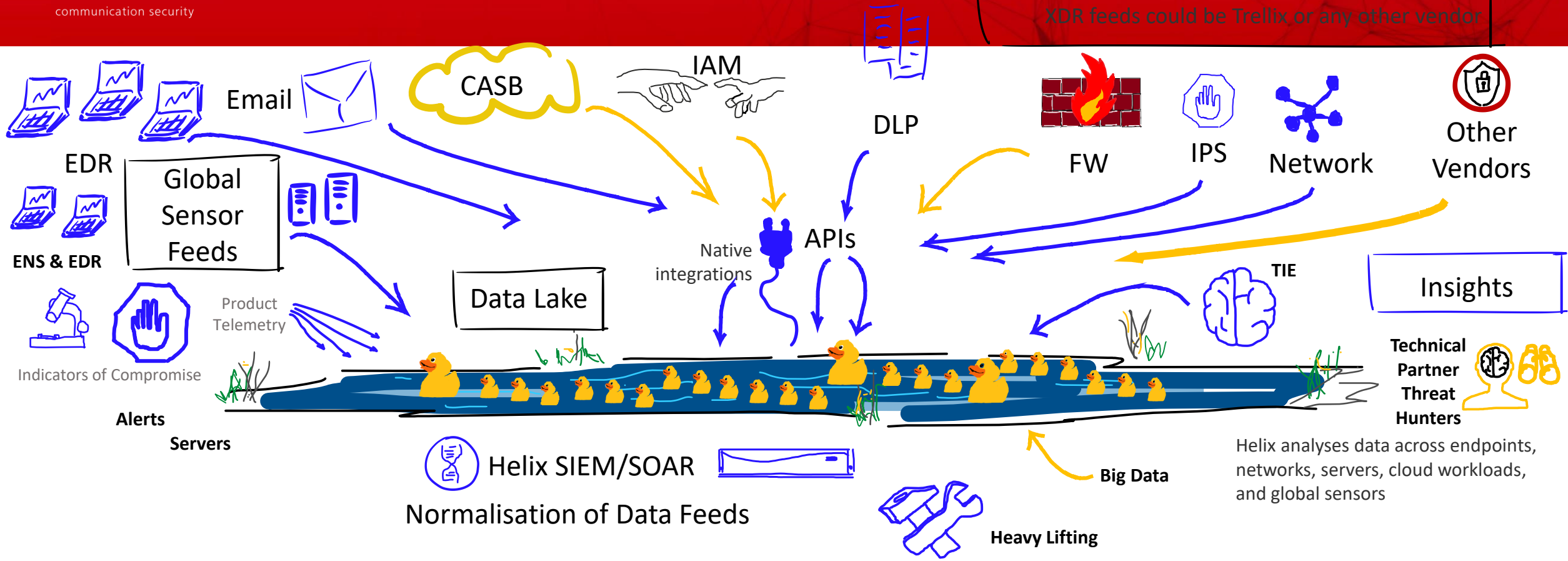
Trellix

XDR feeds could be Trellix or any other vendor



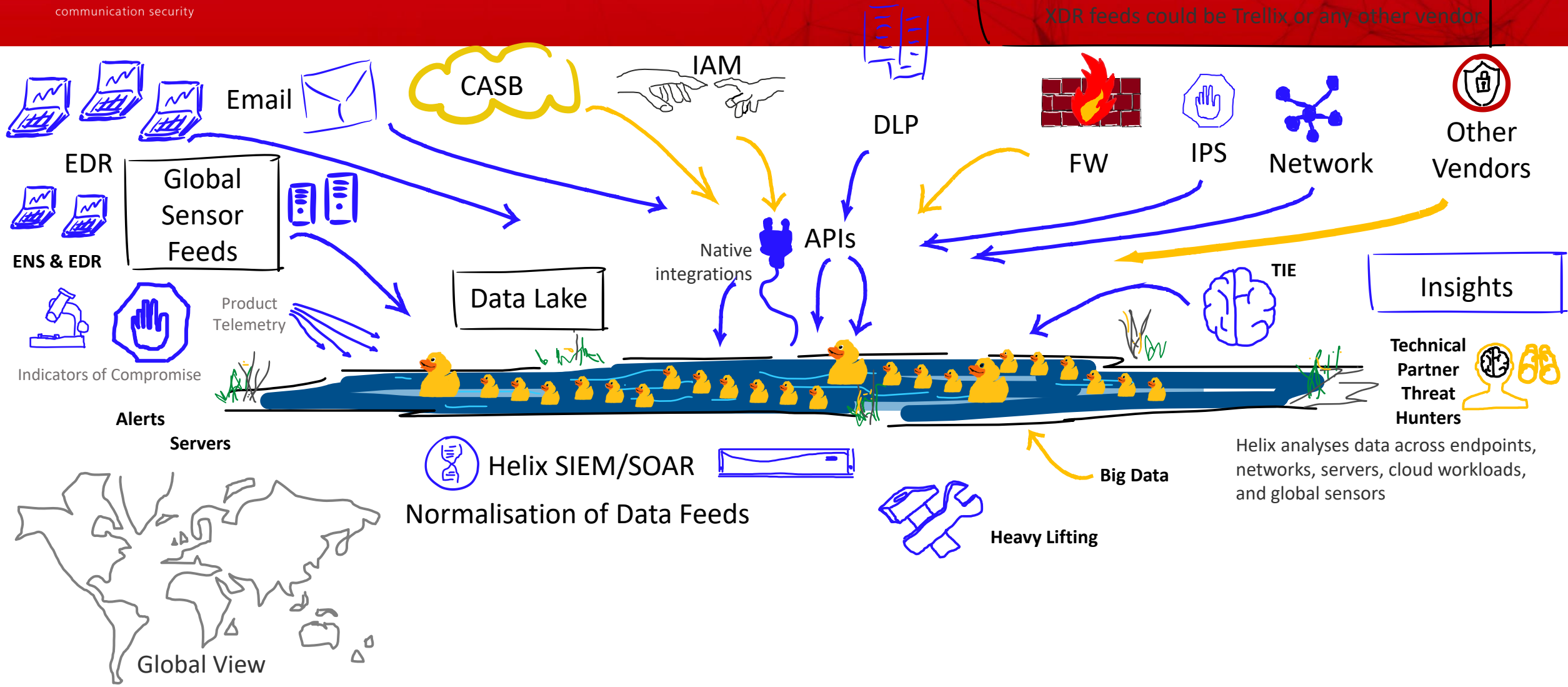
Trellix

XDR feeds could be Trellix or any other vendor



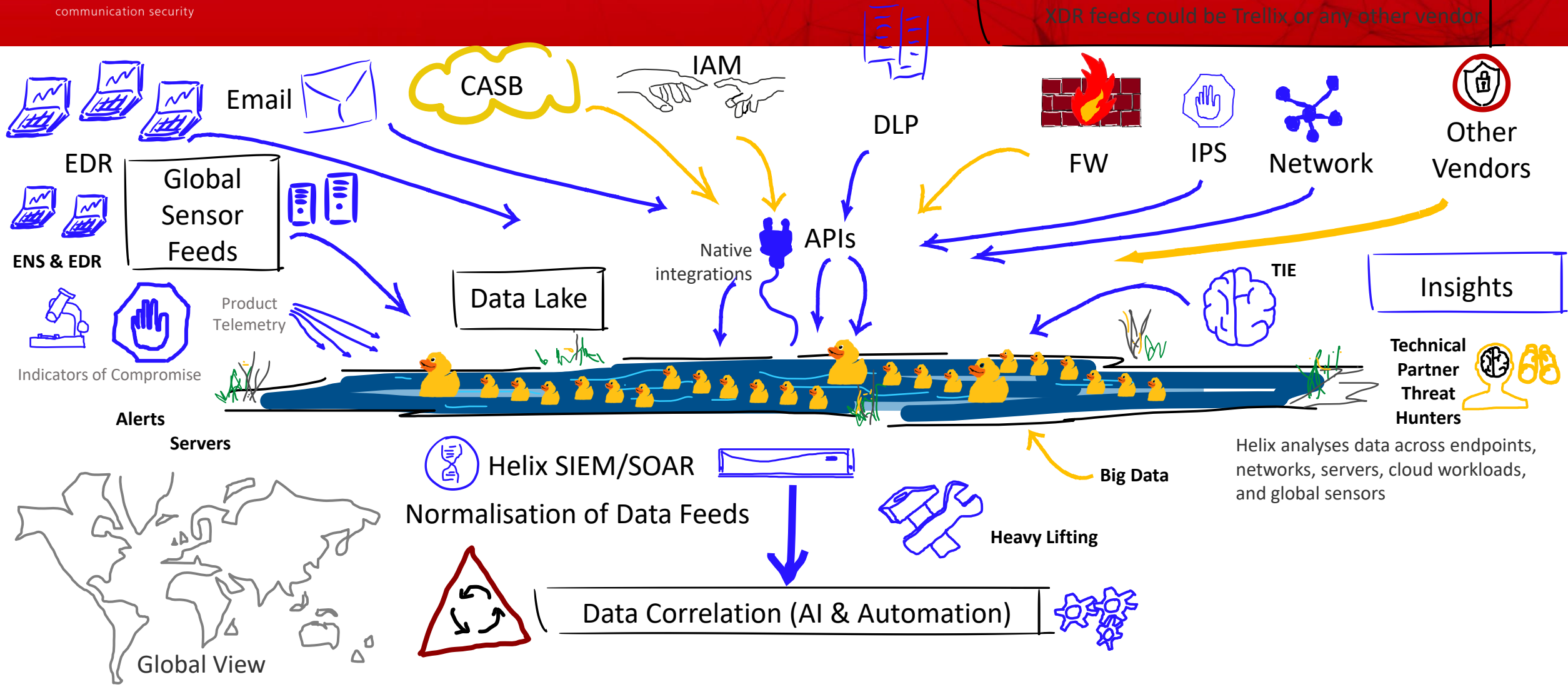
Trellix

XDR feeds could be Trellix or any other vendor



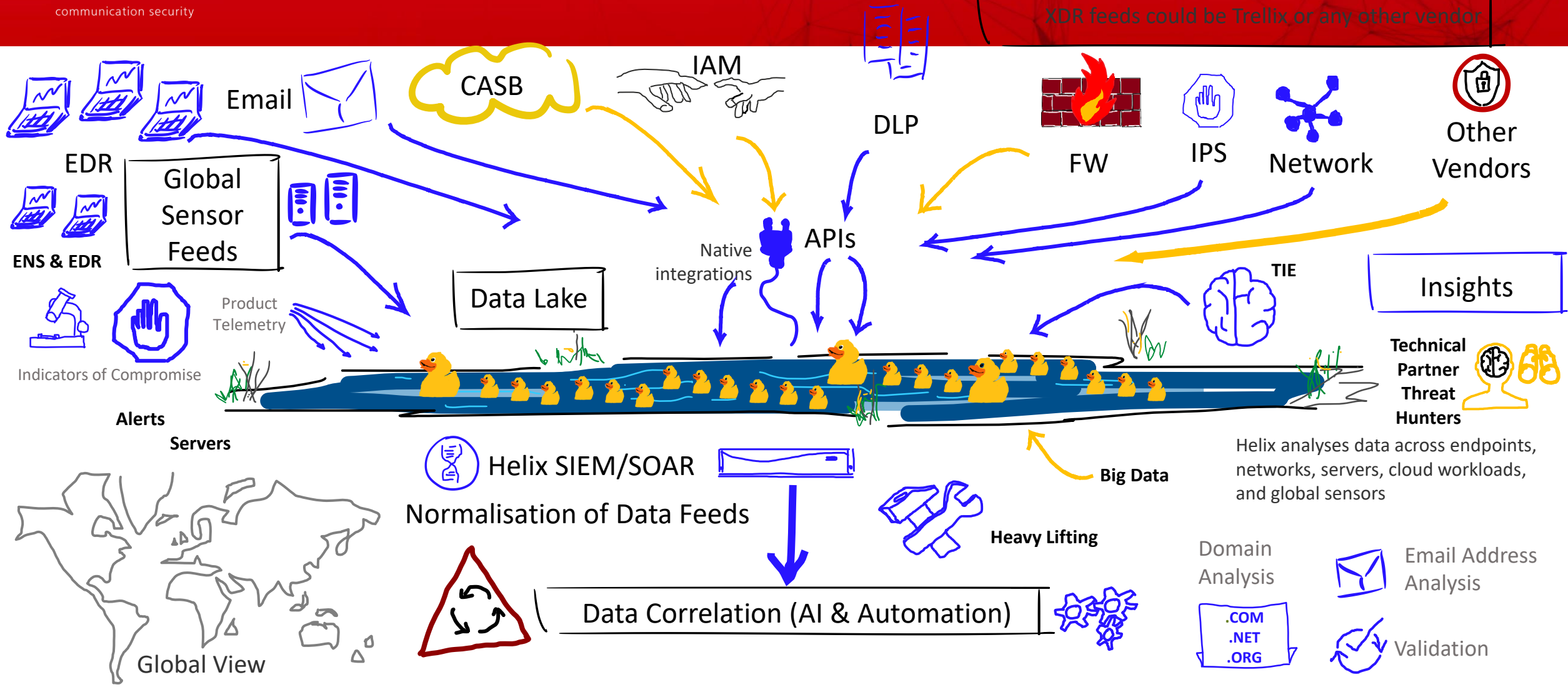
Trellix

XDR feeds could be Trellix or any other vendor



Trellix

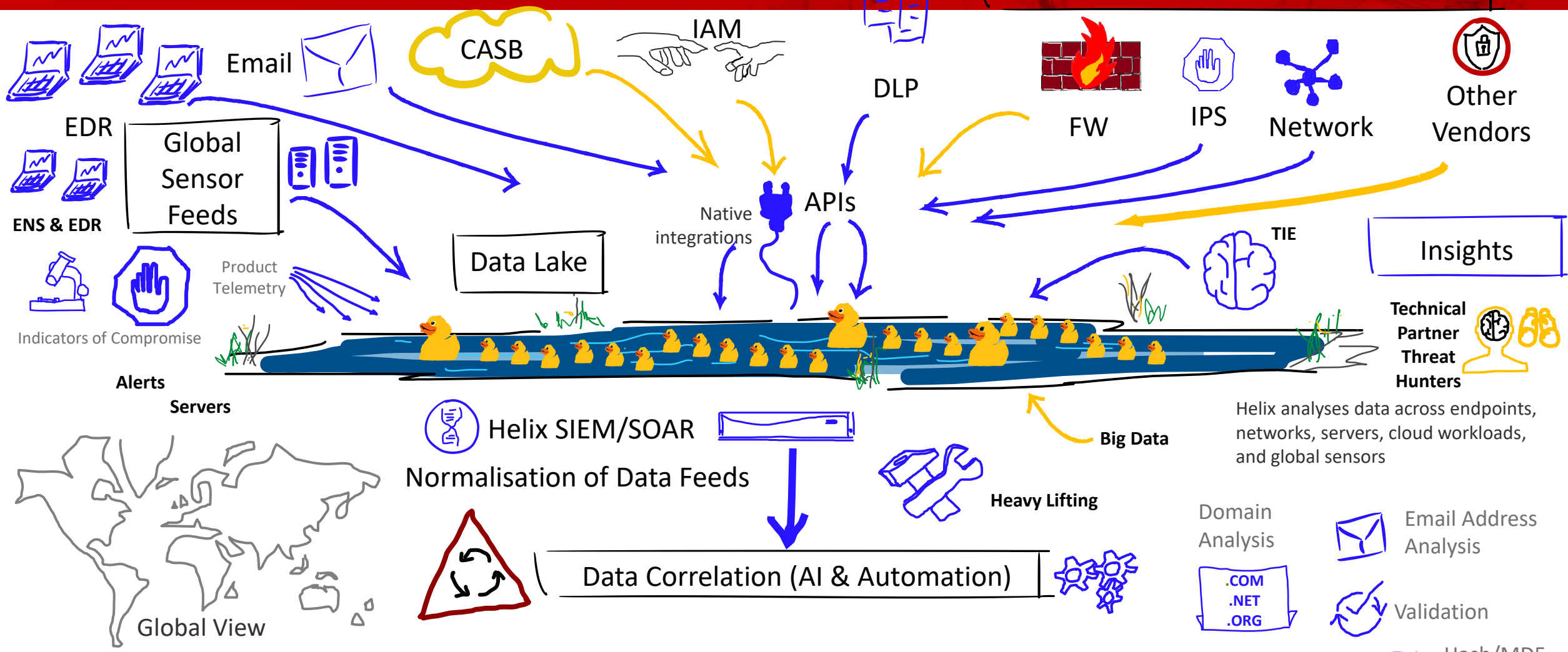
XDR feeds could be Trellix or any other vendor



Trellix

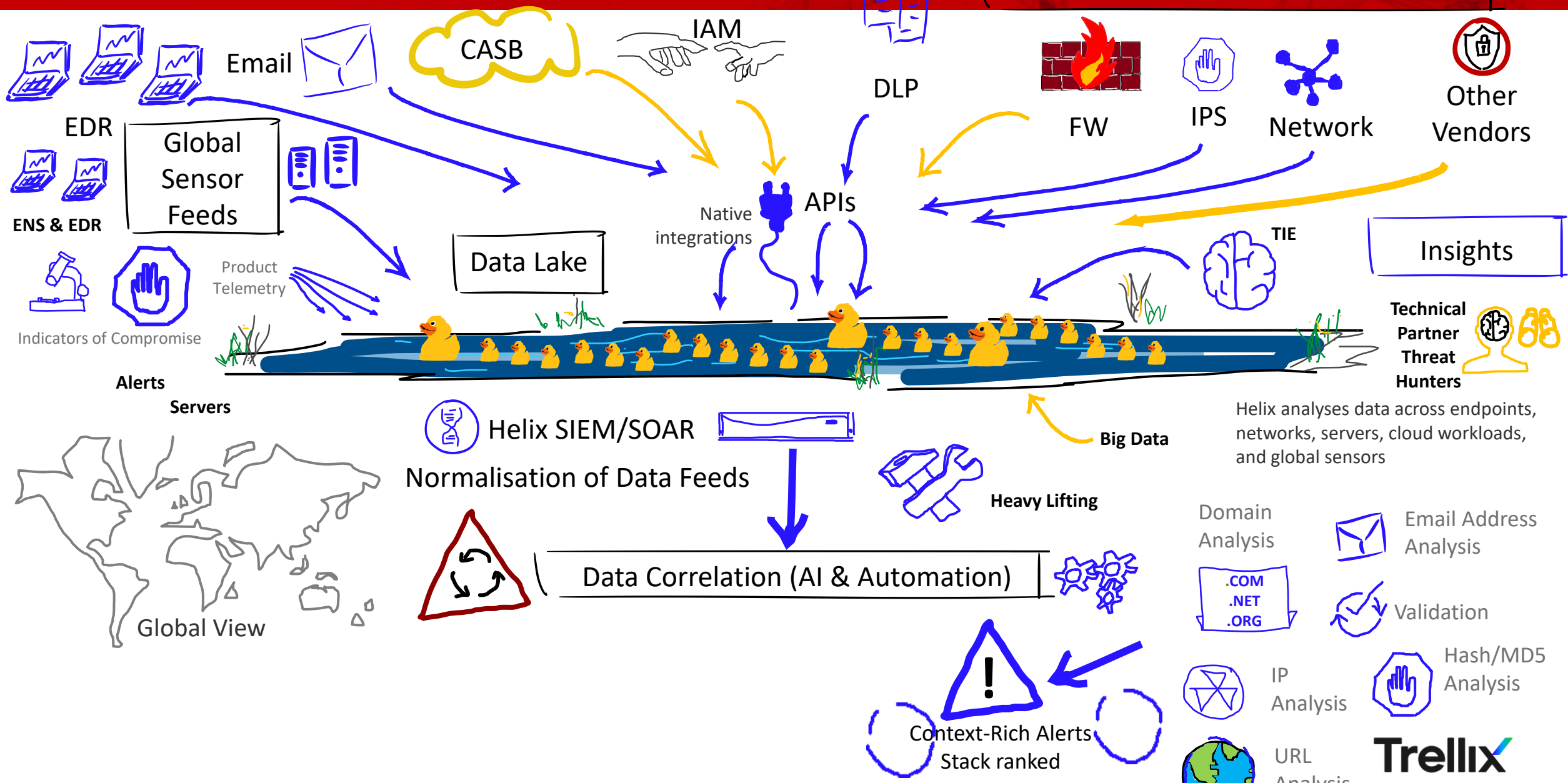
COMGUARD
communication security

XDR feeds could be Trellix or any other vendor



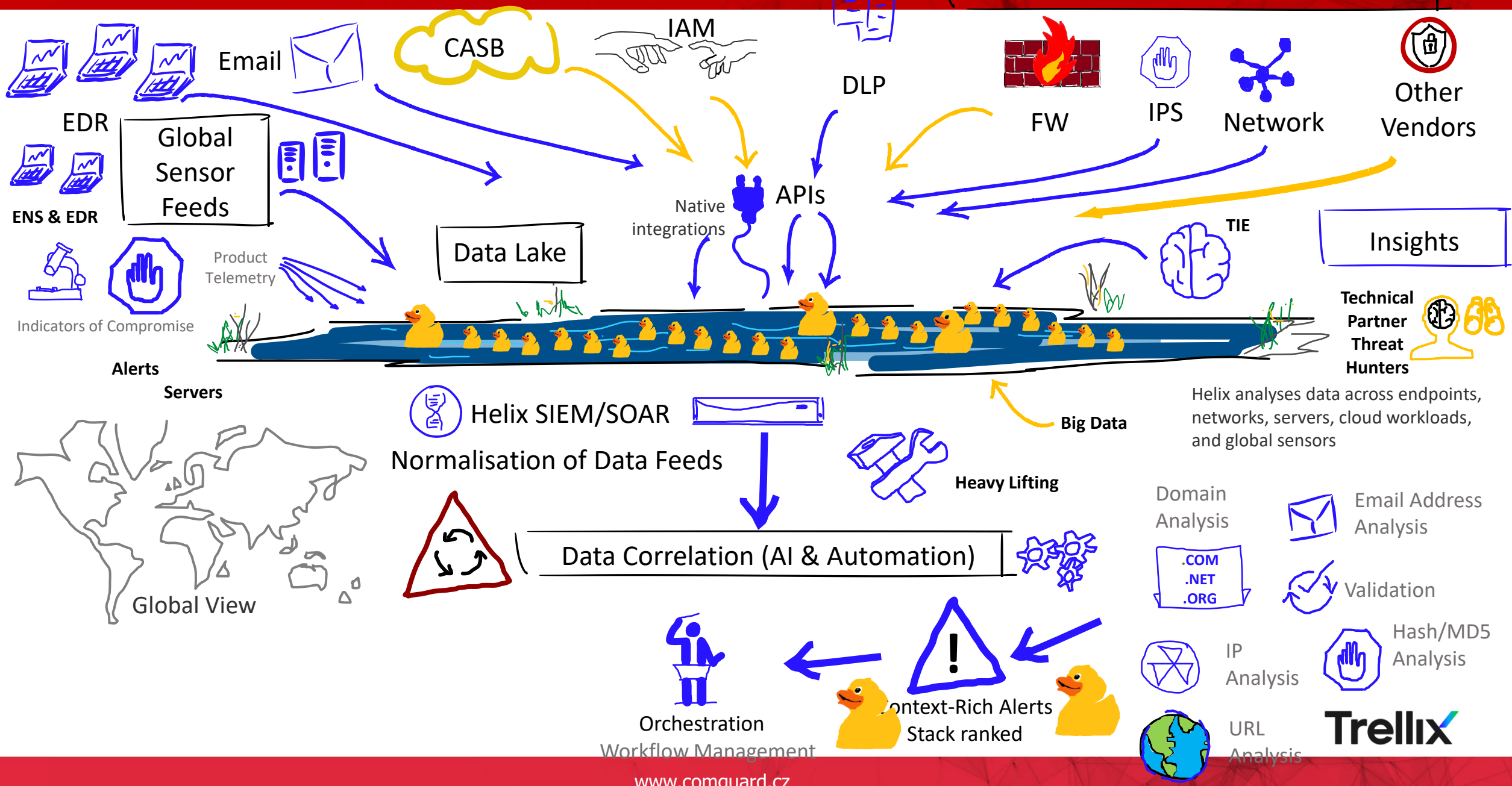
COMGUARD
communication security

XDR feeds could be Trellix or any other vendor



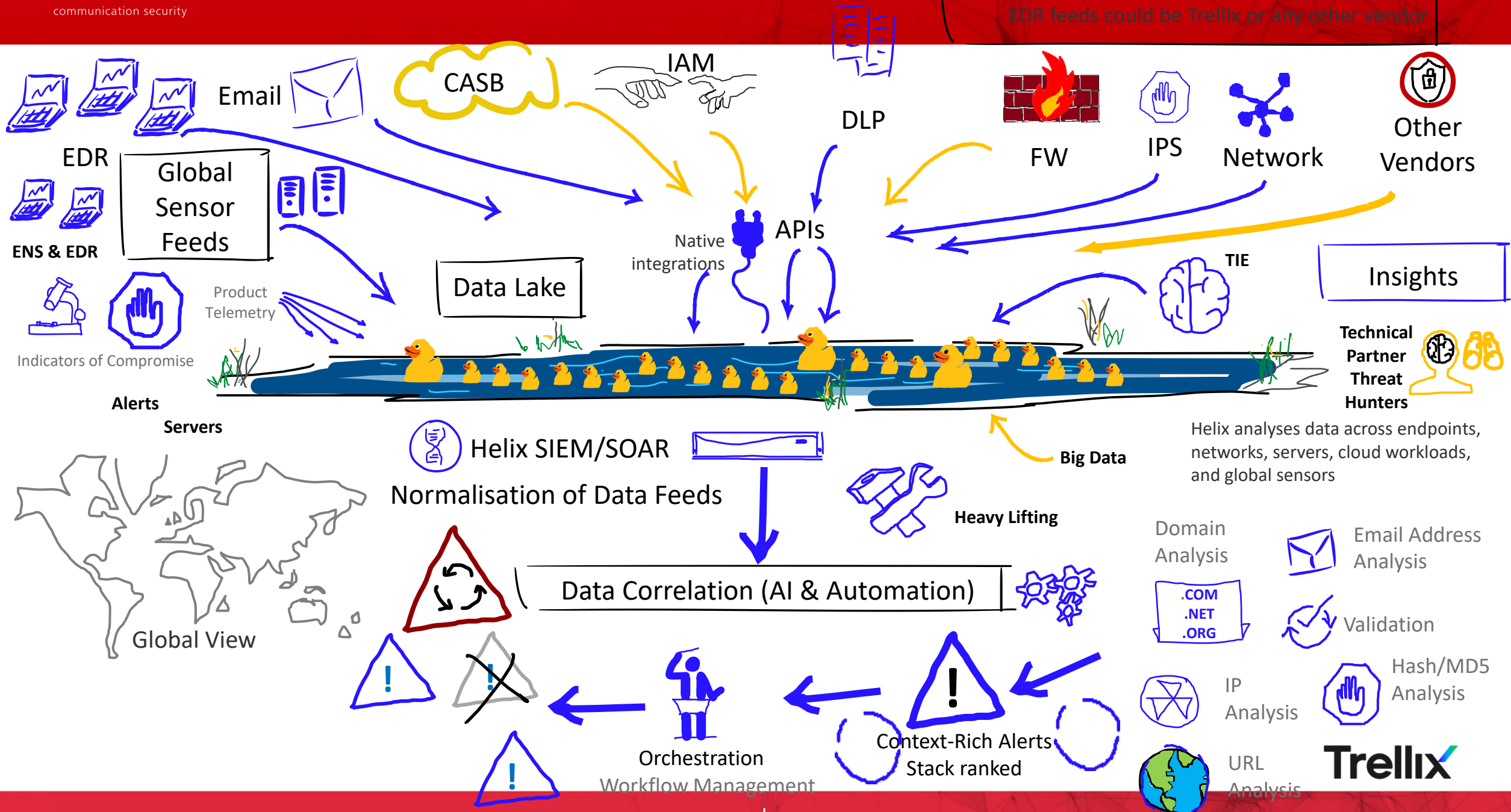
COMGUARD
communication security

XDR feeds could be Trellix or any other vendor



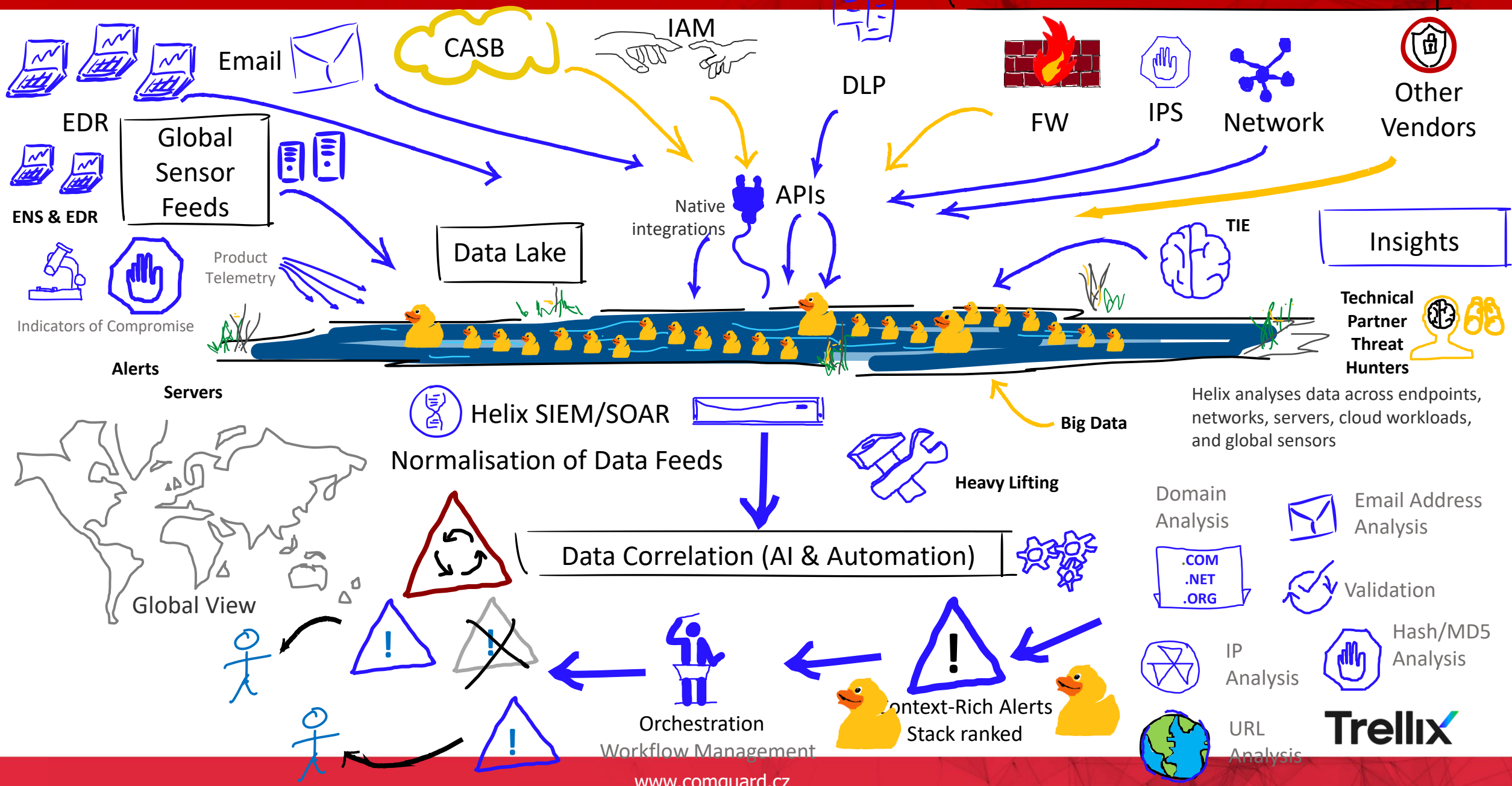
COMGUARD
communication security

XDR feeds could be Trellix or any other vendor



COMGUARD
communication security

XDR feeds could be Trellix or any other vendor



COMGUARD
communication security

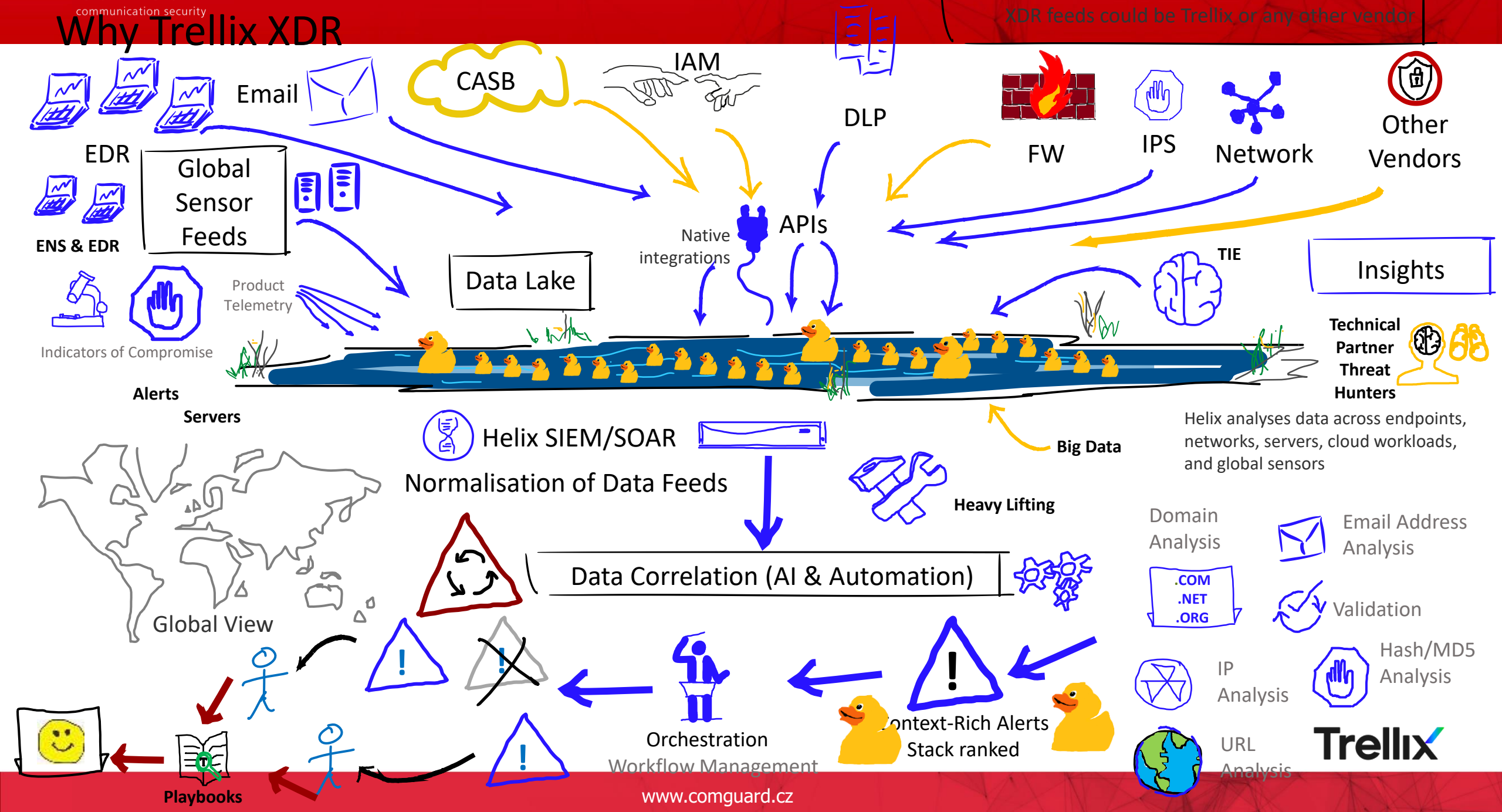
XDR feeds could be Trellix or any other vendor

Email
CASB
IAM
DLP
FW
IPS
Network
Other Vendors
EDR
ENS & EDR
Global Sensor Feeds
Native integrations
APIs
Product Telemetry
Data Lake
TIE
Insights
Indicators of Compromise
Technical Partner Threat Hunters
Alerts
Servers
Helix SIEM/SOAR
Big Data
Helix analyses data across endpoints, networks, servers, cloud workloads, and global sensors
Normalisation of Data Feeds
Heavy Lifting
Global View
Data Correlation (AI & Automation)
Domain Analysis
Email Address Analysis
.COM
.NET
.ORG
Validation
Hash/MD5 Analysis
IP Analysis
URL Analysis
Context-Rich Alerts
Stack ranked
Orchestration
Workflow Management
Playbooks
Trellix

COMGUARD
communication security

Why Trellix XDR

XDR feeds could be Trellix or any other vendor



COMGUARD
communication security

Děkuji za pozornost

Martin.votava@comguard.cz
+420 734 442 468