



Trellix

# Trellix for Defense and Public Sector

Securing Mission-Critical Networks



# Speaker Intro



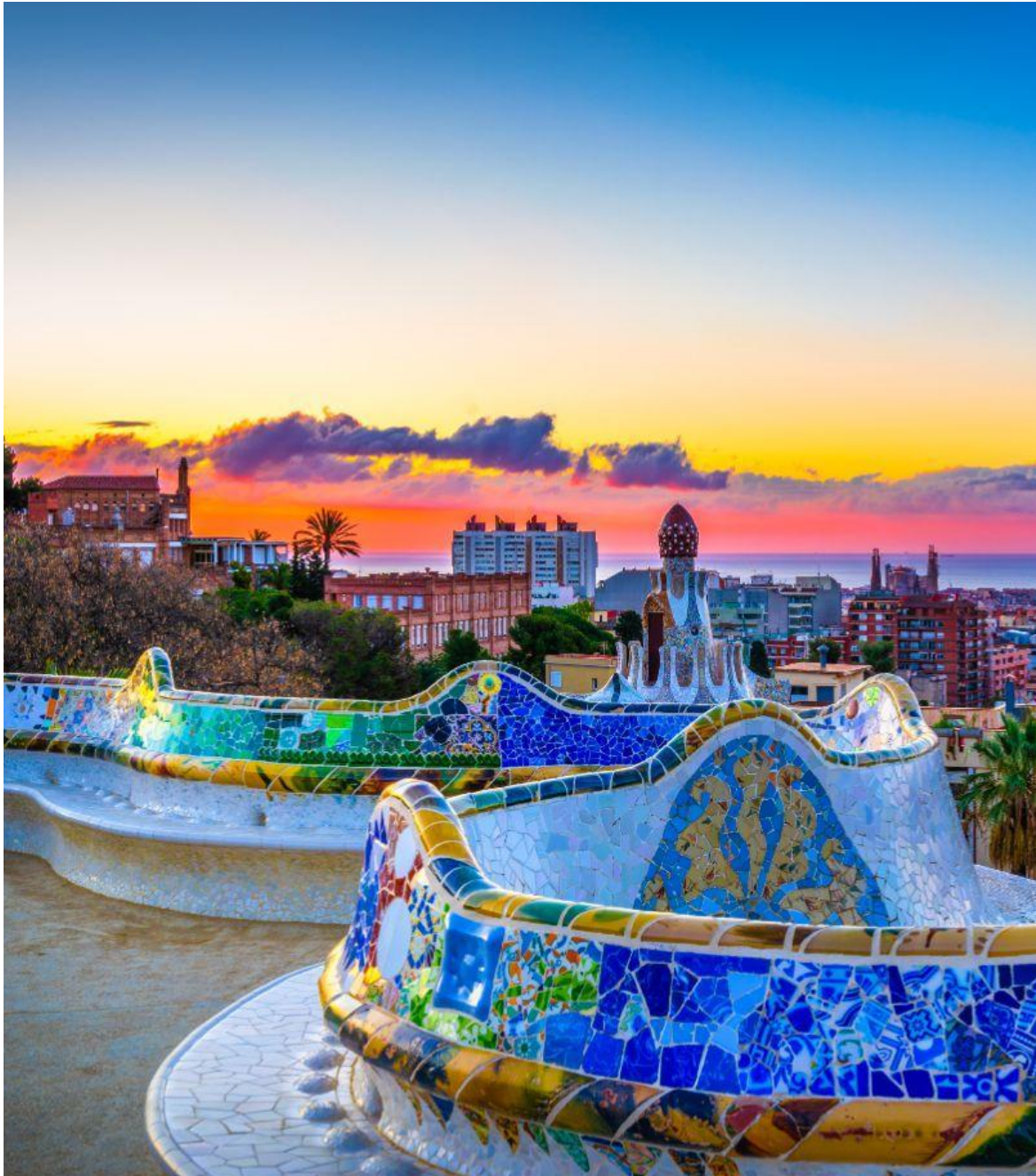
**Ayed Al Qartah**

SecOps Solutions Architect - EMEA



**Siju Ramachandradasan**

Sr. Director Professional Services



# Agenda

- Introduction
- Securing Email
- Threat Intelligence
- Zero Trust
- Data Security
- Air Gapped Networks
- Trellix XDR Reference Architecture
- Q & A

# 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.



# Securing Email



# Current Situation: Why the need?

There is no such thing as a safe email

## Primary Attack Vector



91% of cyberattacks begin with spear phishing\*\*\*

## Cloud Email Adoption



70% of organizations use cloud email solutions and growing\*\*

## Microsoft isn't good enough



3M attacks missed by Microsoft in a year across 1058 customers\*

## Average breach lifecycle



277 days resulting from business-email compromise\*\*\*\*

\*Trellix Advance Research Center | \*\*Gartner Market Guide for email security | \*\*\*Knowbe4.com Nov 29, 2022 | \*\*\*\*IBM Cost of a Data Breach Report 2022

# The Anatomy of HTML Attachment Phishing: One Code, Many Variants

By [Mathanraj Thangaraju](#), [Niranjan Hegde](#), and [Sijo Jacob](#) · June 14, 2023

## Introduction

Phishing is the malevolent practise of pretending sensitive data, such as login credentials or credit card numbers, due to how easy it is for bad actors to execute an email attachment. HTML files are one of the most common attachments used in phishing attacks. Some email security filters and are often seen as legitimate files, but they can be executable files.

# The Psychology of Phishing: Unraveling the Success Behind Phishing Attacks and Effective Countermeasures

By [Tomer Shloman](#) · February 1, 2024

# Cybercrooks Leveraging Anti Automation Toolkit for Phishing Campaigns

By [Vihar Shah](#) and [Rohan Shah](#) · December 18, 2023

## Peeling the Hidden Layers

By [Neel H. F.](#)

## Introduction

Malicious actors have noticed an increase in phishing attacks steadily going up. The primary motivation is mostly device and URL

Threat actors have a track record of abusing tools hosted on GitHub for malicious purposes. Last year we showed how attackers [abused Python's tarfile module](#). Trellix Advanced Research Center has tracked abuse of one more such tool used for quite some time now. [Predator](#), a tool designed to combat bots and web crawlers, can distinguish web requests originating from automated systems, bots, or web crawlers.

This blog will show how cybercriminals have abused this GitHub tool, and how this tool has been used in multiple phishing campaigns with frequently changing url patterns in a very short span.

ity  
eyond  
and

# Trellix Email Security

How we do it...Better

## Full Threat Detection Efficacy



Unmatched threat detection: cloud-based multi-tenant advance URL defense and attachment detonation



Comprehensive protection against numerous attack vectors



Block threats and provide contextual insights to prioritize and accelerate response

## Integrated Investigation and Response



Detect and prioritize threats to help quick remediation of advanced threats



Remediation capabilities to automatically or manually pull email out in inboxes post delivery



Prioritize, correlate, and remediate emails from SEC Op's platform

## Comprehensive and Resilient



Secure Email Gateway or behind existing solution



Native integration into MS365 and Google Workspace

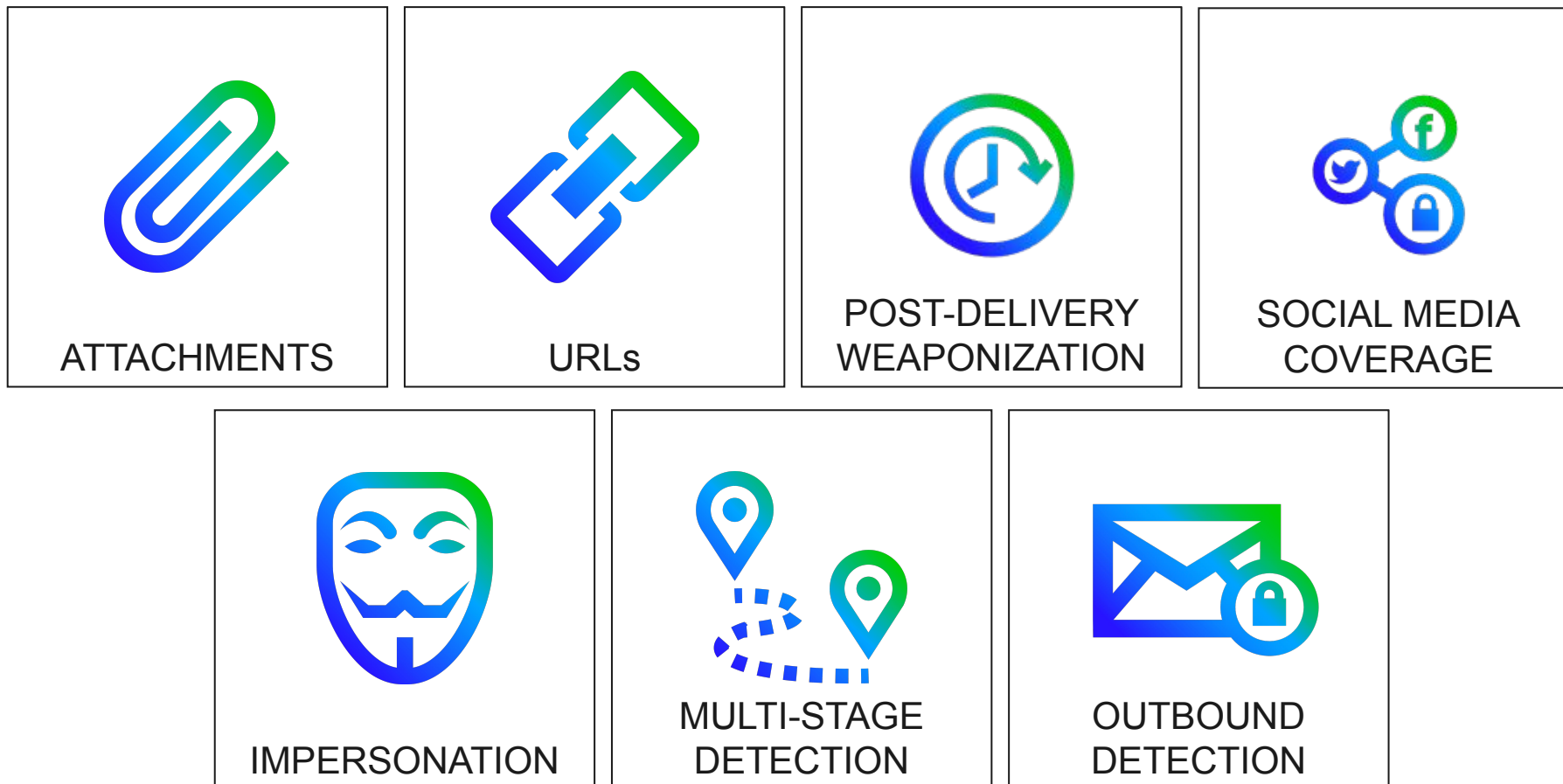


Telco grade resiliency

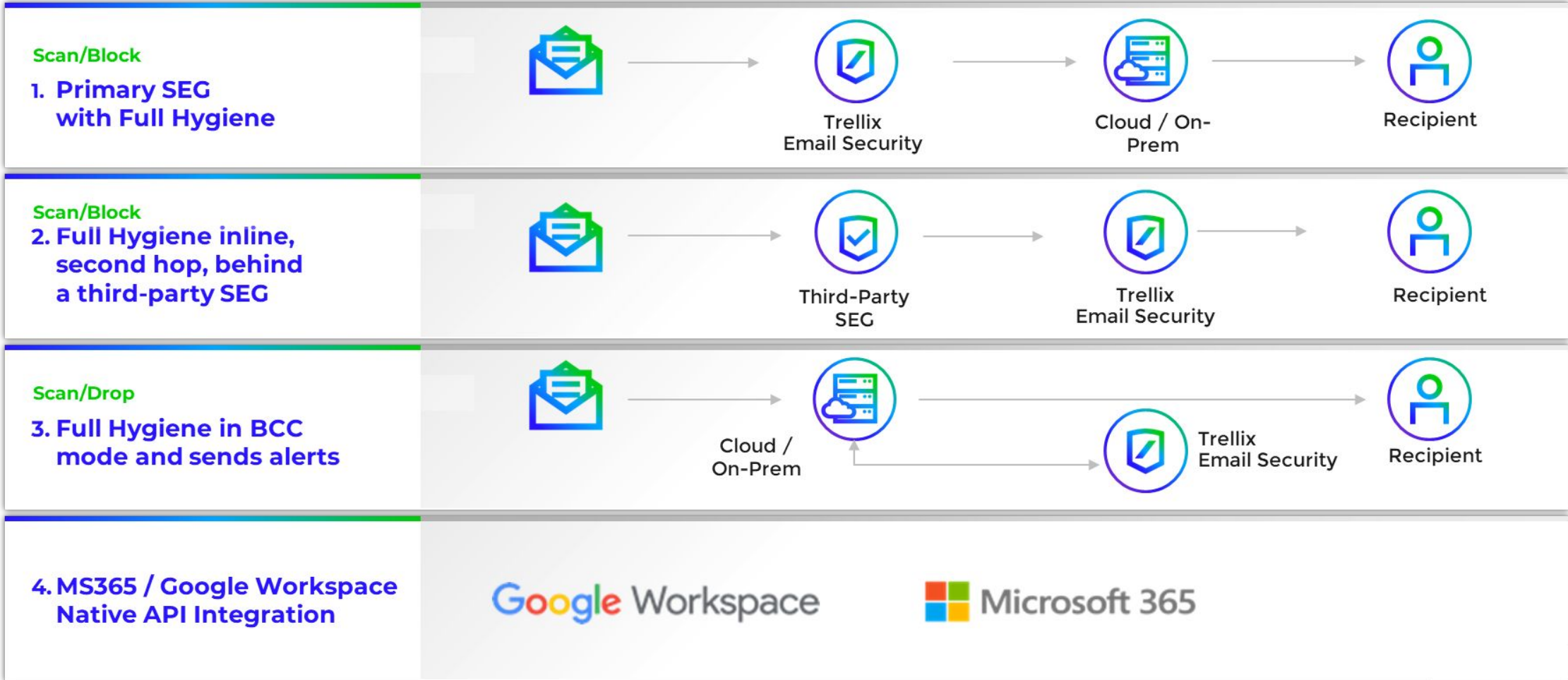


# We catch what others miss

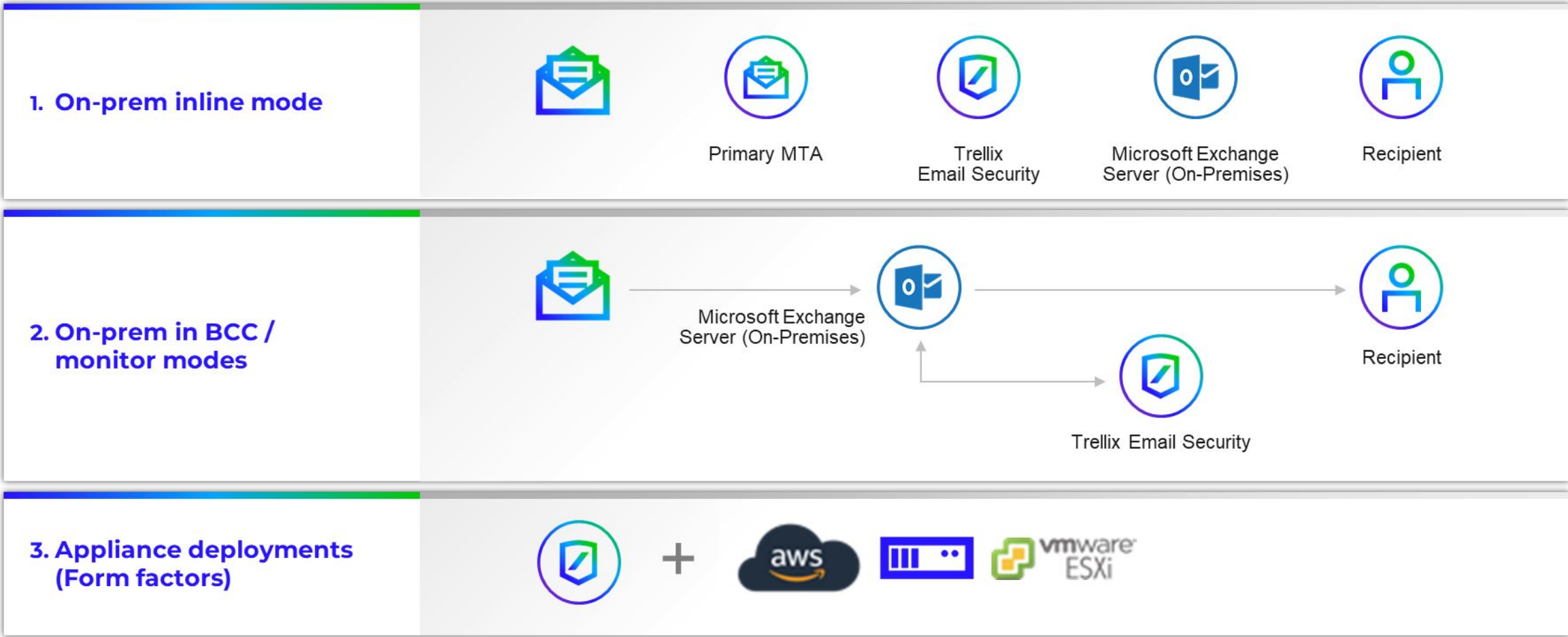
Trellix identifies and blocks all email threat categories



# Flexible Deployment Cloud Email



# Flexible Deployment Server Email

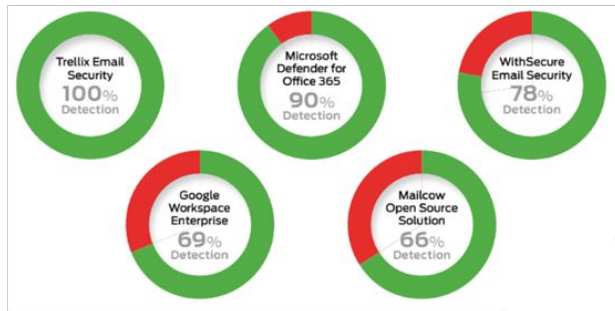


# Superior Detection Proven by Third-Party Testing

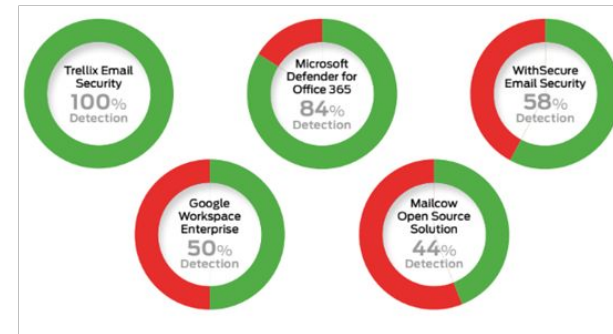
## Beating Microsoft and Google



### #1 in Detection



### #1 in Accuracy



# Threat Intelligence



# Operational Threat Intelligence Foundation



JOINT CYBER DEFENSE  
COLLABORATIVE



**1.5 PB**

of data (samples)

**8.75 TB**

data processed  
per day

**2B**

email samples  
per day

**250M**

malicious file detections  
per month

**Real-time,  
reliable,  
information  
to:**

1. Anticipate threats
2. Detect and block threats
3. Accelerate informed responses

# Trellix Threat Intelligence Solutions

One of the broadest and deepest intelligence offerings on the market

Millions of sensors distinctly across key vectors (endpoint, email, web, & network)

Cloud and OnPrem Deliverable

**Trellix**

Global Threat Intelligence (GTI)

Trellix Insights

Trellix Intelligence Exchange (TIE)

Intelligence as-a-Service

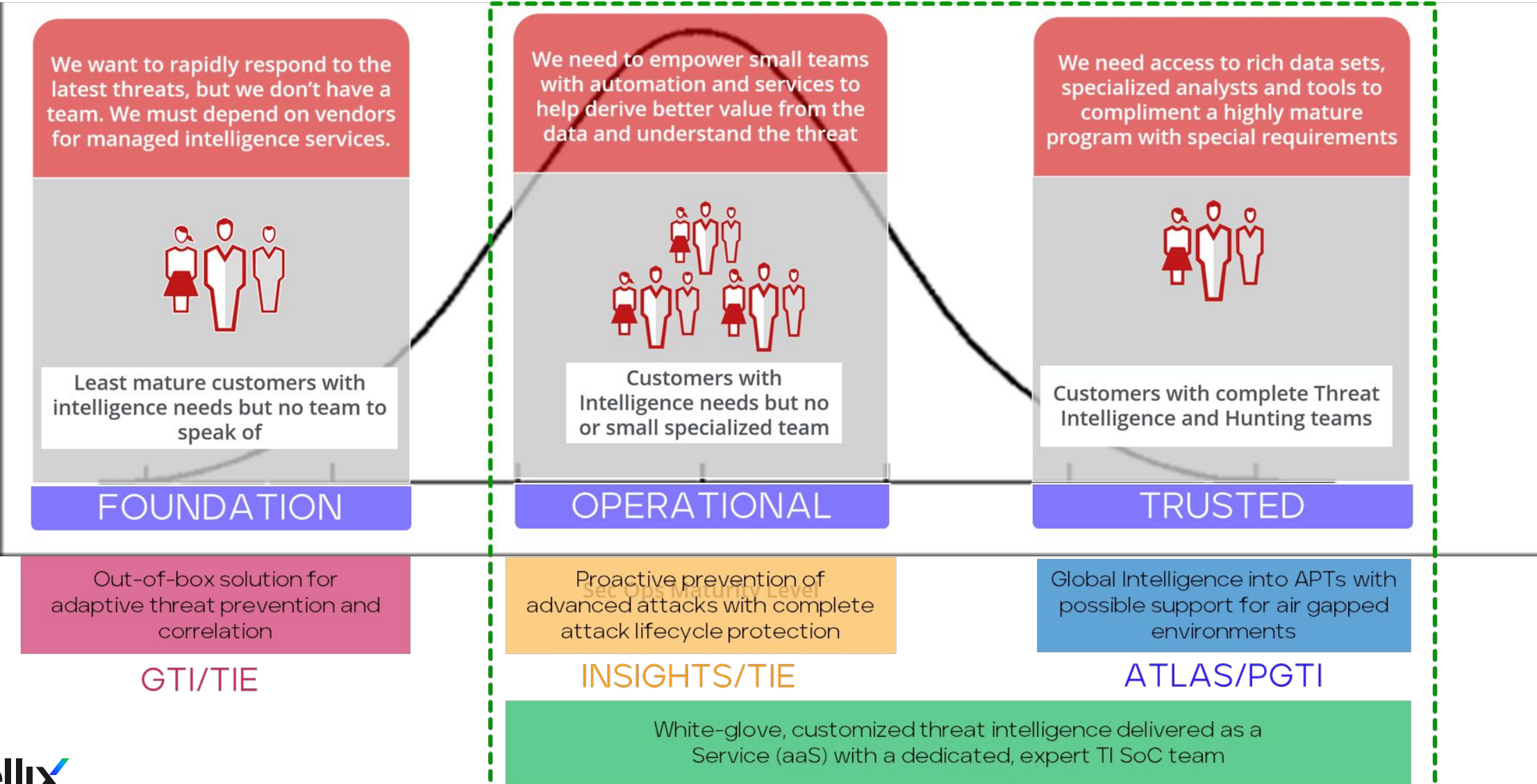
Advanced Threat Landscape Analysis System (ATLAS)

Private GTI



<https://www.trellix.com/en-us/platform/threat-intelligence.html>

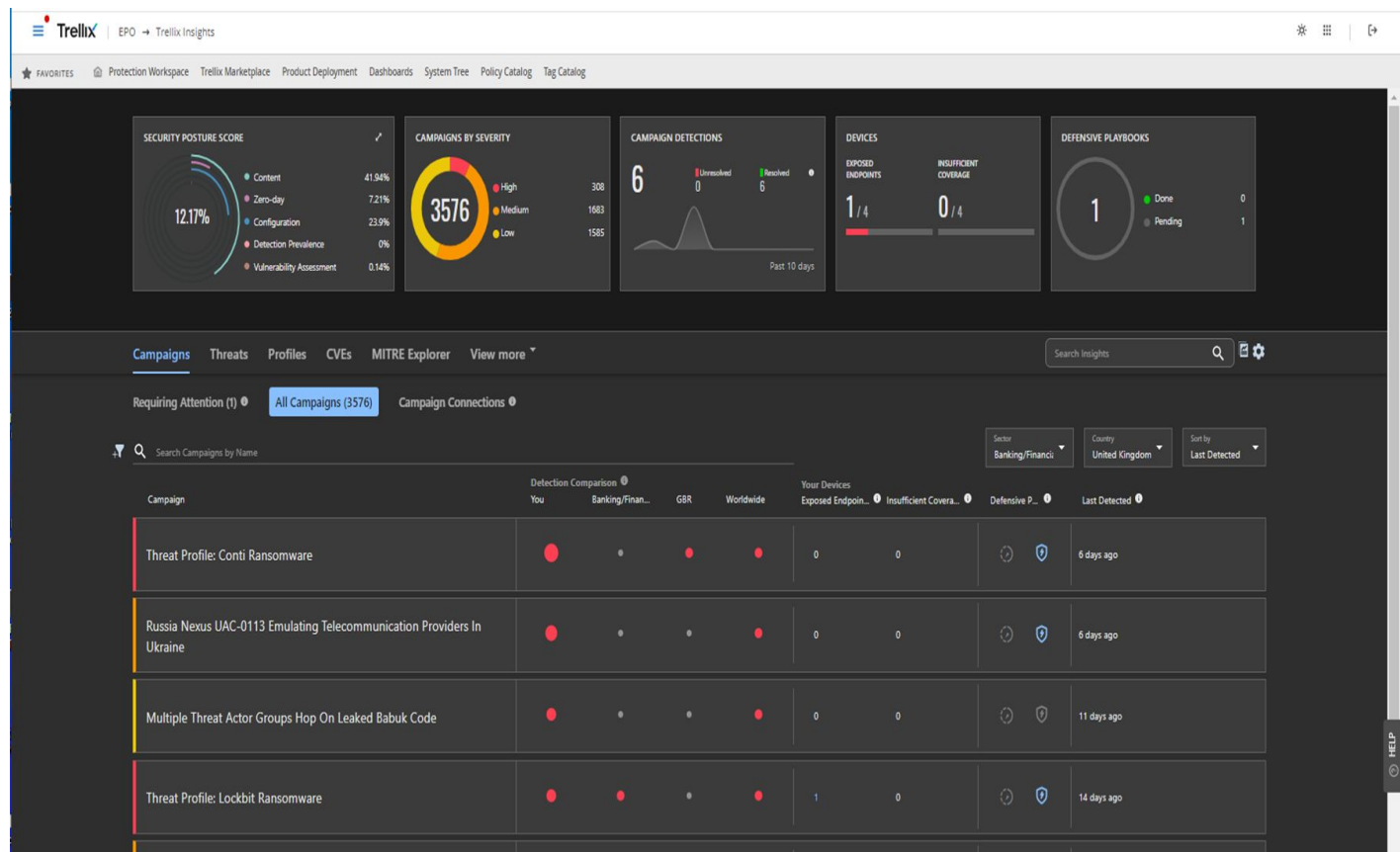
# Threat Intel Needs by Sec Ops Maturity





# Trellix Insights

- Predict threats likely to hit your organization based on one billion sensors globally and machine team analysis from the ARC team.
- Prioritize threats based on an assessment of your security gaps, know how your security will perform and how you stack up against your peers
- Preemptively act with prescribed countermeasures



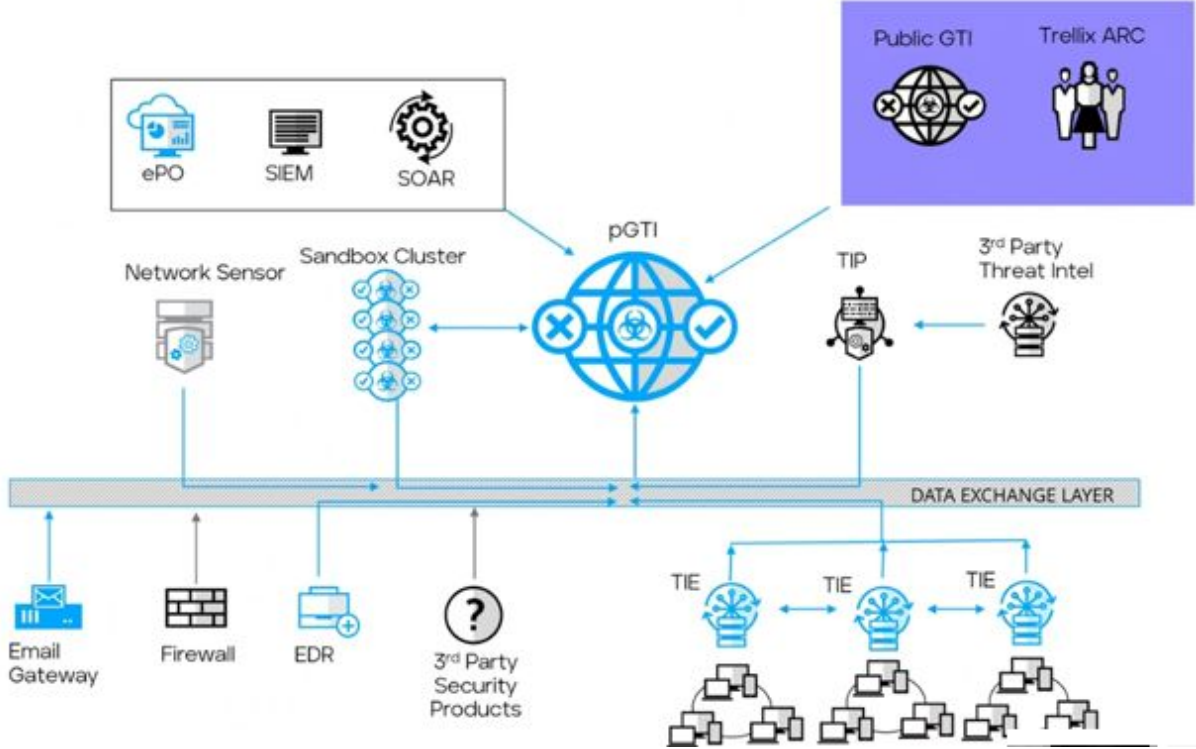
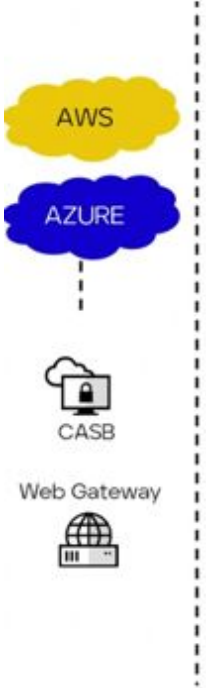
# Advanced Threat Landscape Analysis System

- Unique global insight into the malicious threat detections seen worldwide by Trellix.
- Utilize the Trellix telemetry data collected worldwide.
- View current and emerging threats by highlighting those of particular interest by type, industry sector, geolocation, most seen, etc.
- Access to a dedicated view for campaigns consisting of events, dates, threat actors, IOCs, threat tools, threat categories, MITRE ATT&CK patterns, countries, and more.



# Private Global Threat Intelligence (pGTI)

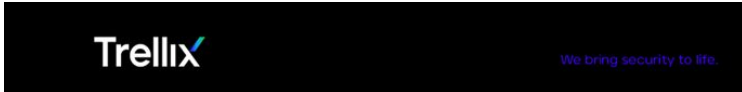
- Trellix File/IP/URL reputations are now available within private or air-gapped environments.
- Private GTI can store up to 10 million of your reputations that supersede Public GTI reputations.
- Complete access to your Private GTI query logs for advanced analytics to discover advanced threats.
- Analysts have access to billions of File/IP/URL reputations through a web-based and command-line interface.



# Intelligence as-a-Service (INTaaS)

✓ **Comprehensive threat intelligence analysis, including:**

- Threat actor or Group attribution and TTP analysis.
- Threat Intelligence driven Risk assessments.
- Threat Intelligence analyst augmentation using multiple sources and tools.
- Malware analysis – Static or Dynamic limited reversing
- Malicious Infrastructure analysis
- Underground engagements and monitoring
- Enrichment from Telemetry and previous Trellix reporting
- Tailored Threat briefings
- Social network analysis.
- Ability to understand and isolate high impact events like network or customer compromises.



TLP: GREEN

We bring security to life.

### Table of Contents

Table of Contents.....	1
General Overview.....	2
Data acquisitions and unpacking techniques .....	3
Icedid malware.....	5
Javascript (Stage 2).....	5
Powershell script (Stage 3).....	5
.NET DLL analysis (Stage 4).....	6
Icedid malware (Stage 5) configuration .....	7
Features.....	11
Cobalt Strike beacon.....	13
Payload execution.....	13
Javascript (Stage 2).....	13
Powershell script (Stage 3).....	13
.NET DLL analysis (Stage 4).....	14
Cobalt Strike beacon (Stage 5) configuration.....	15
Features.....	18
Conclusion.....	19
IoCs.....	20
Icedid.....	20
Hashes.....	20
C2 IP.....	20
Registry key.....	20
Cobalt Strike.....	21
Hashes.....	21
C2 IP.....	21
Persistence.....	21
Registry key.....	21
Appendix.....	23
Bibliography.....	23



the second most similar to the to it.<sup>4</sup>

ected by any dress.

# Trellix Zero Trust Strategy

Never Trust, Always Verify



# 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>



# 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**

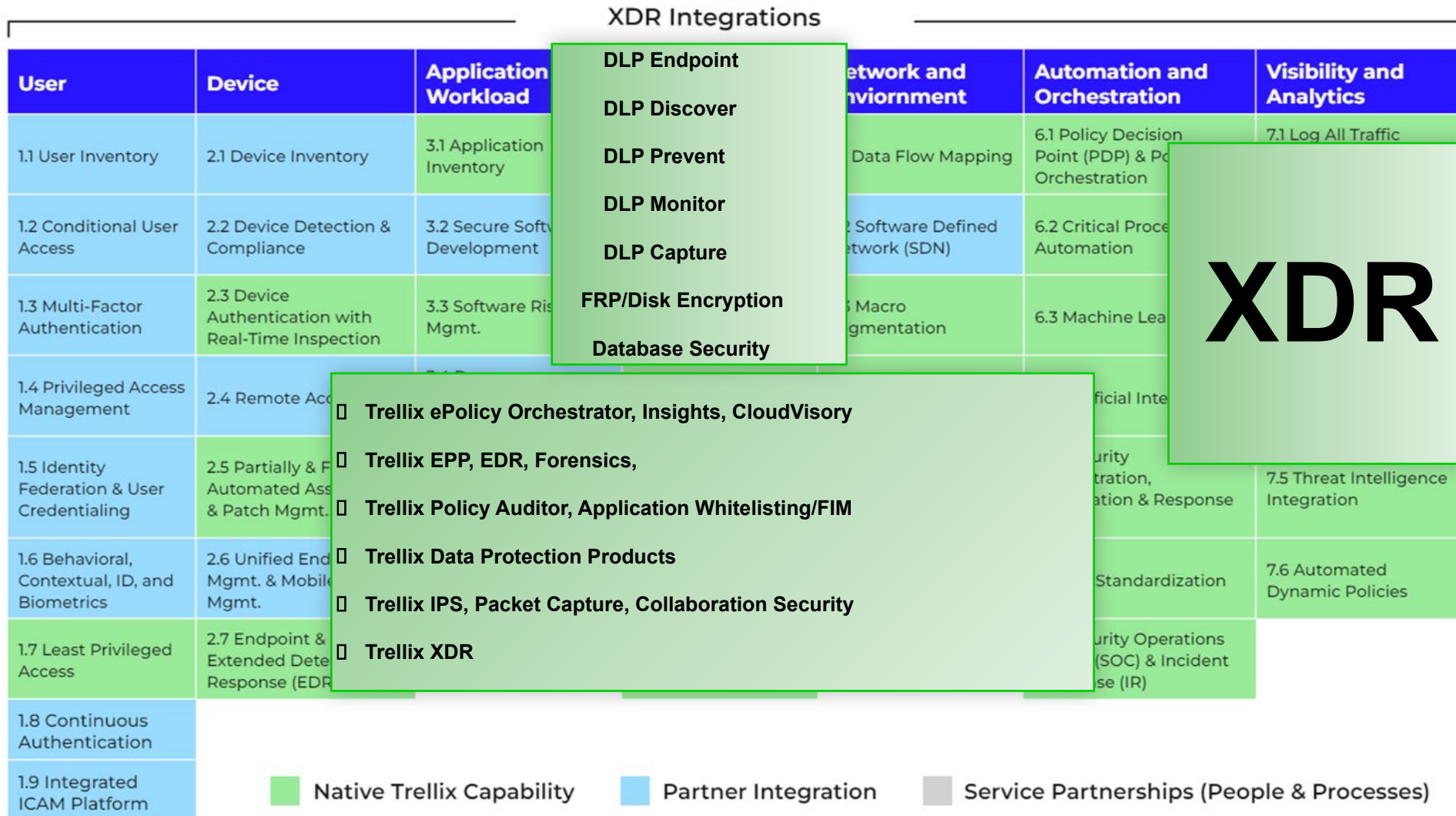
4

**Prioritize and automate SecOps workflows across all controls**

5

**Aggressive development and partnership to meet ZT requirements**

# XDR aligns the DoD's 7 Pillars of Zero Trust

















# Data Security

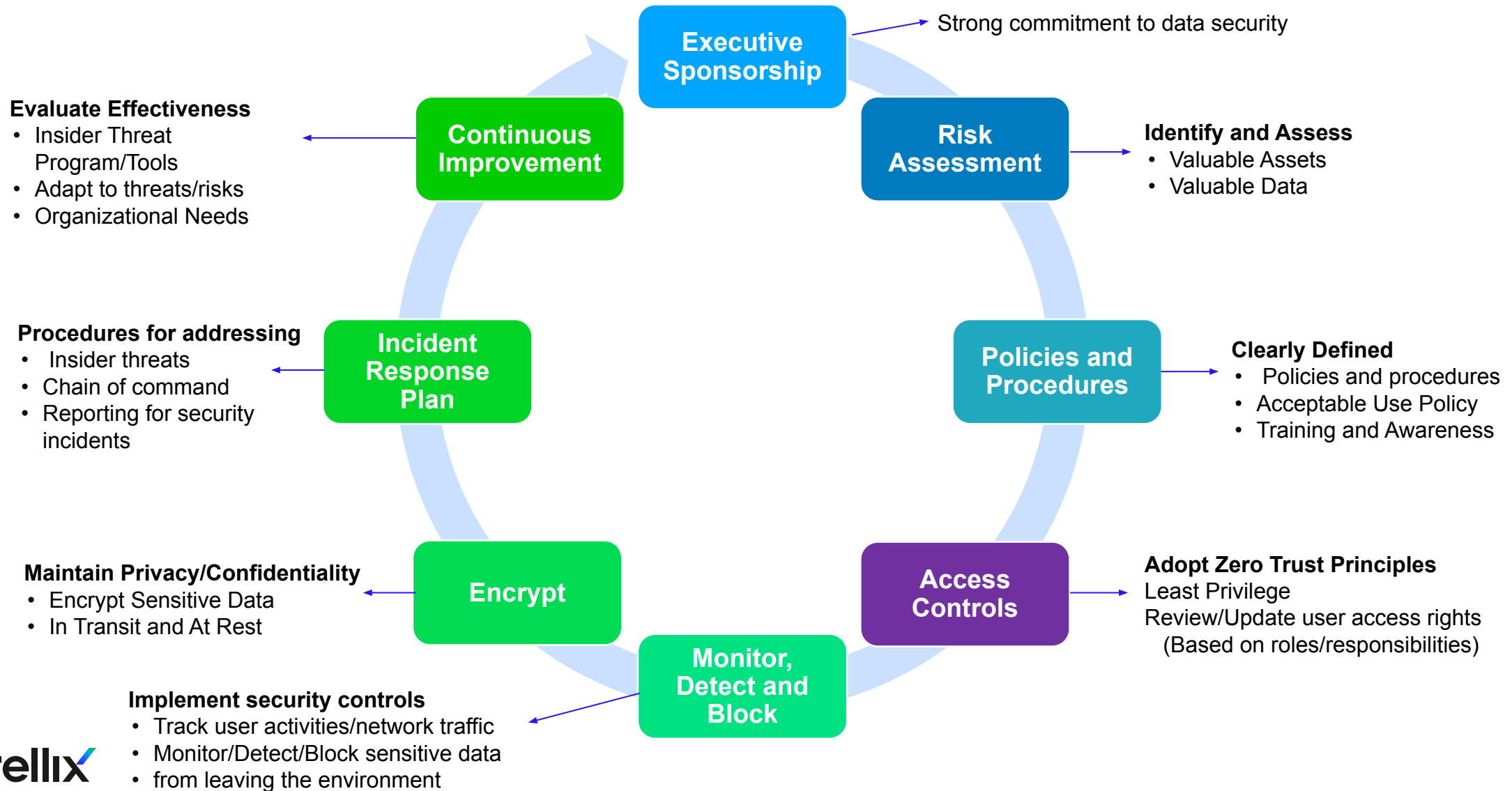


# Key Data Security Challenges

Addressing Multiple Use Cases – Across Multiple Vectors

Insider Risk		 Visibility, Control, Close Loop remediation, Response
Data Privacy	 	 Data at rest, Data in use, Data in motion
Governance, Risk, Compliance		 Management of business plans/strategies, Risks that impact operations, Adherence to standards, laws, and regulations
External Threat/Forensics	 	 Context in a multi-vector attack, visibility across the cyber attack kill-chain, Forensic Investigation and response
Zero Trust Architecture		 Access control, Least Privilege, Air-gapped environments

# Data Security Key Pillars



# Comprehensive Visibility, Unified Control



Data on the Endpoints



Data in the Network



Data in the Database



Data in the Cloud

## Discover

- More than 300 content types
- Self-remediation scan option
- On-premise and in the cloud

## Classify

- Manual
- Automated
- 3rd party integrations

## Protect

- Create user awareness
- Multiple vectors
- Customizable reports

# Trellix Data Security

## Mapping to Zero Trust Architecture Requirements

### ZTA Requirements

Cover data-at-rest,  
in-motion, in-use  
4.1

Data is tagged w/  
required criteria  
4.2

Access control  
mechanisms based  
on tagging  
4.3

Data Monitoring  
4.4

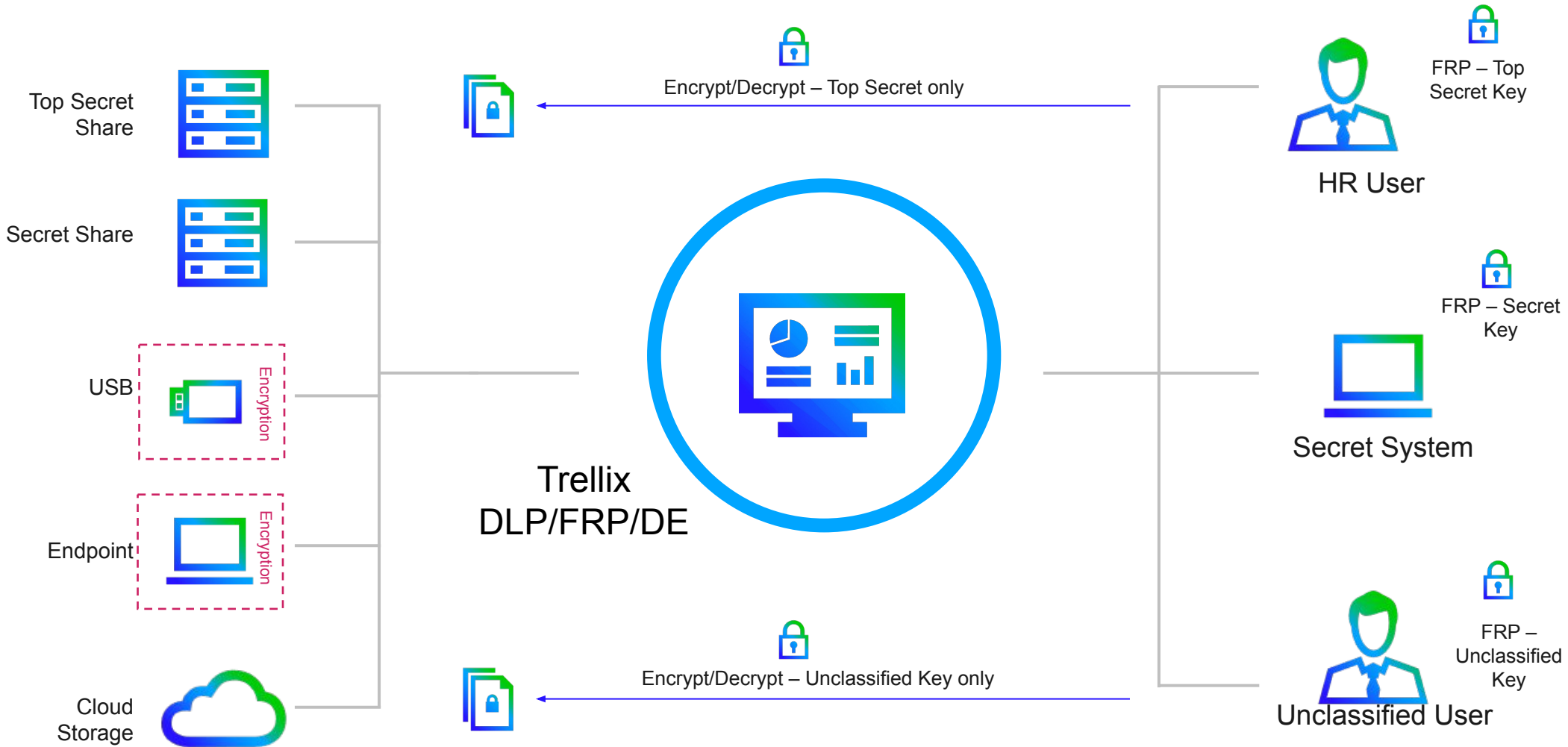
Data Encryption and  
DRM  
4.5

DLP  
4.6

- ✓ DLP Endpoint and DLP Network Multi-Vector Protection Rules
- ✓ File and Folder Level Encryption
- ✓ Data Classification, Tagging, DRM
- ✓ Policies based on classification

# Zero Trust – Data Pillar

Control – 4.2 Data Governance, 4.5 Data Encryption and Rights Management



# Zero Trust - Data Pillar

Control – 4.2 Data Governance, 4.3 Data Labeling & Tagging

**Inventory**

- Scan network for file shares
- Inventory files



DLP Discover

**Classify**

- Automatic/Manual
- Structured/Unstructured
- Integrations
  - MIP, Titus, Bolden James



On Premise Sharepoint



File Shares/Box



Databases

**Fingerprint**

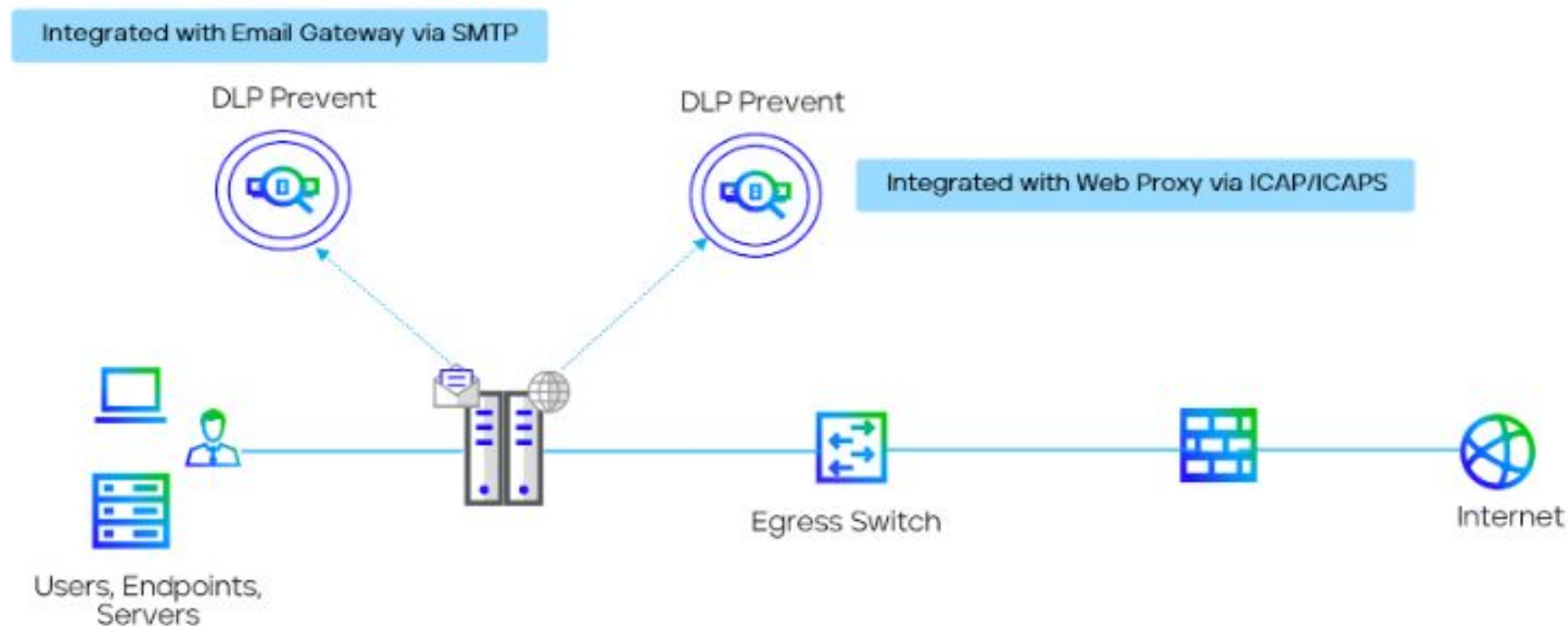
- Structured/Unstructured
- Exact Data Matching

**Remediate**

- Copy/Move
- Apply Rights Management
- Classify

# Zero Trust - Data Pillar

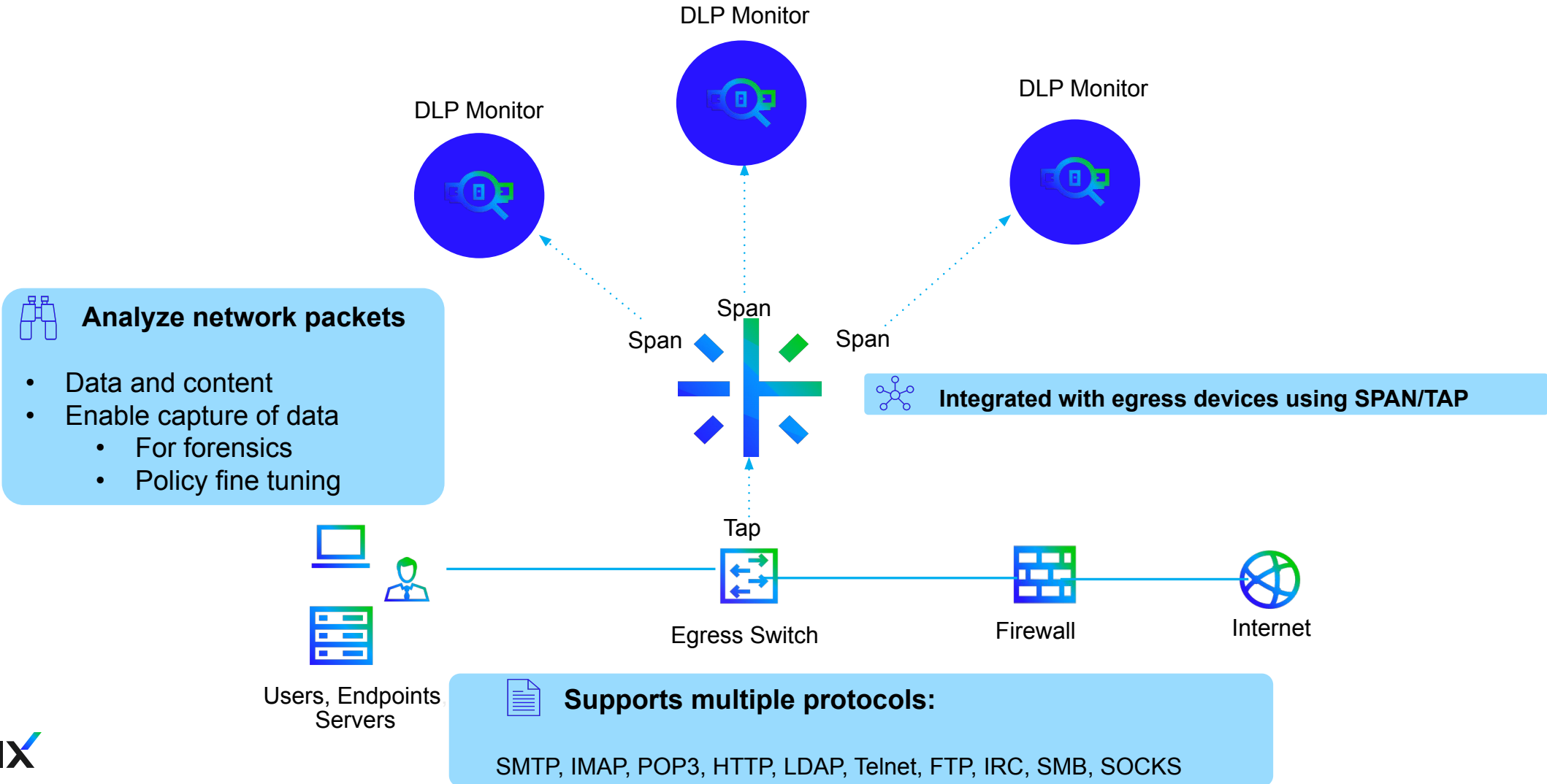
Control - 4.4 Data Monitoring, 4.6 Data Loss Prevention





# Zero Trust – Data Pillar

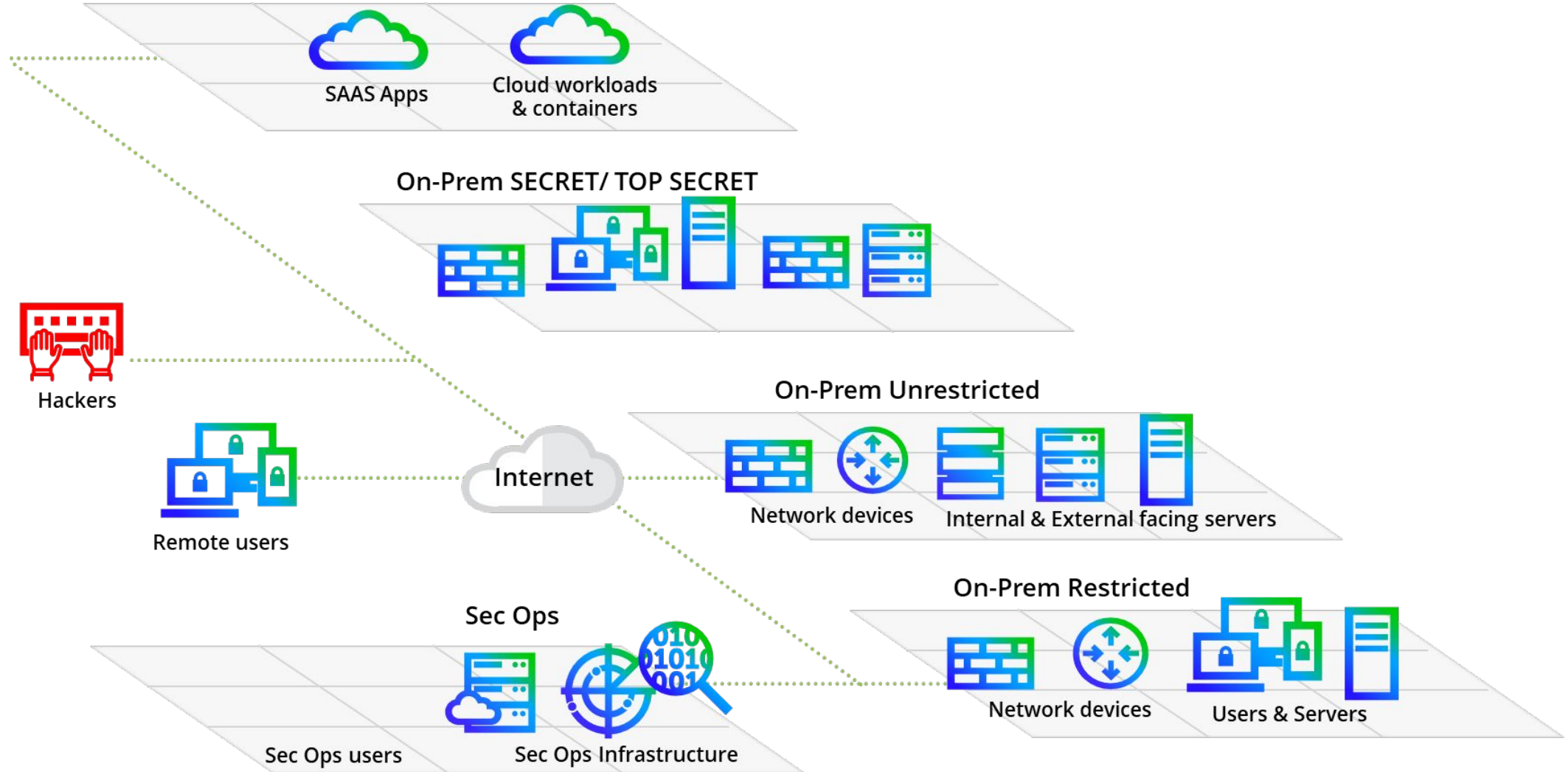
Control – 4.2 Data Governance, 4.4 Data Monitoring



# Air-Gapped Networks



## Internet and Cloud Services

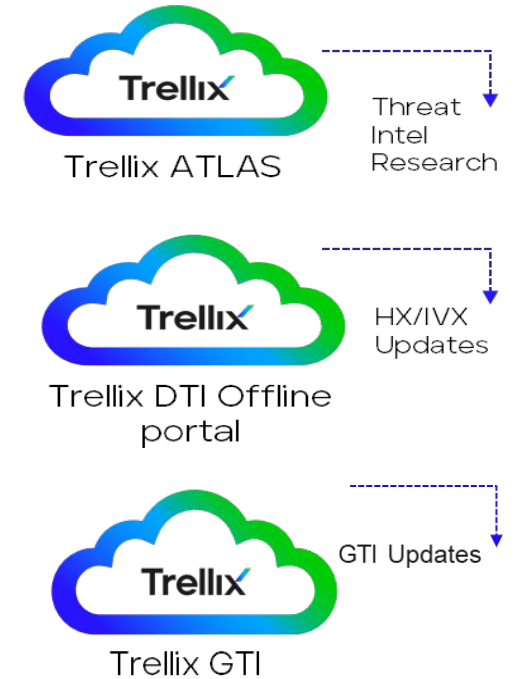
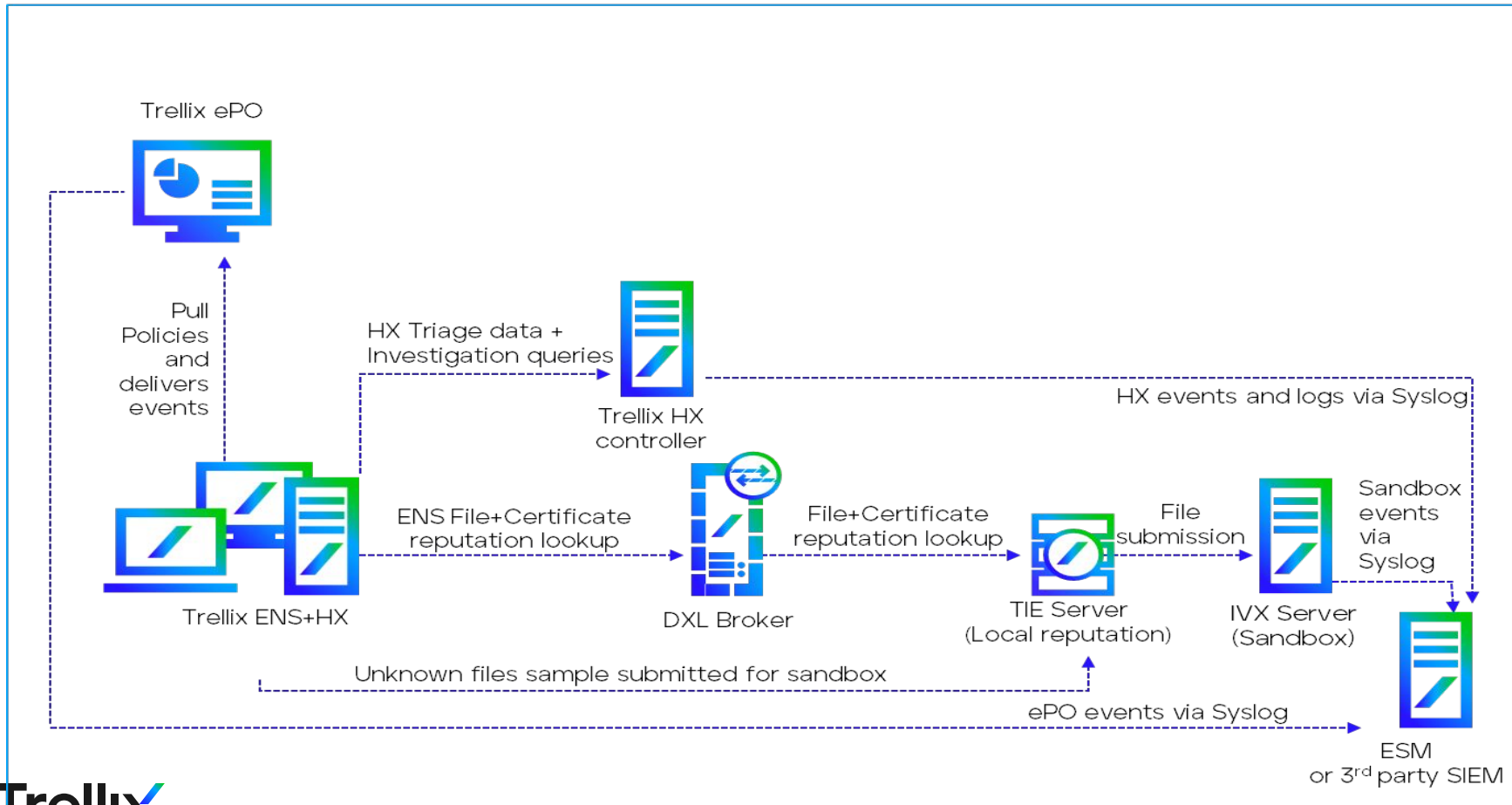


# On-Premises Solutions

- Endpoint Security, Forensics
- DLP, Encryption, Device Control
- Malware Sandboxing
- Network Security (IPS, Advanced Threat Protection)
- Application Control
- Threat Intelligence
- SIEM

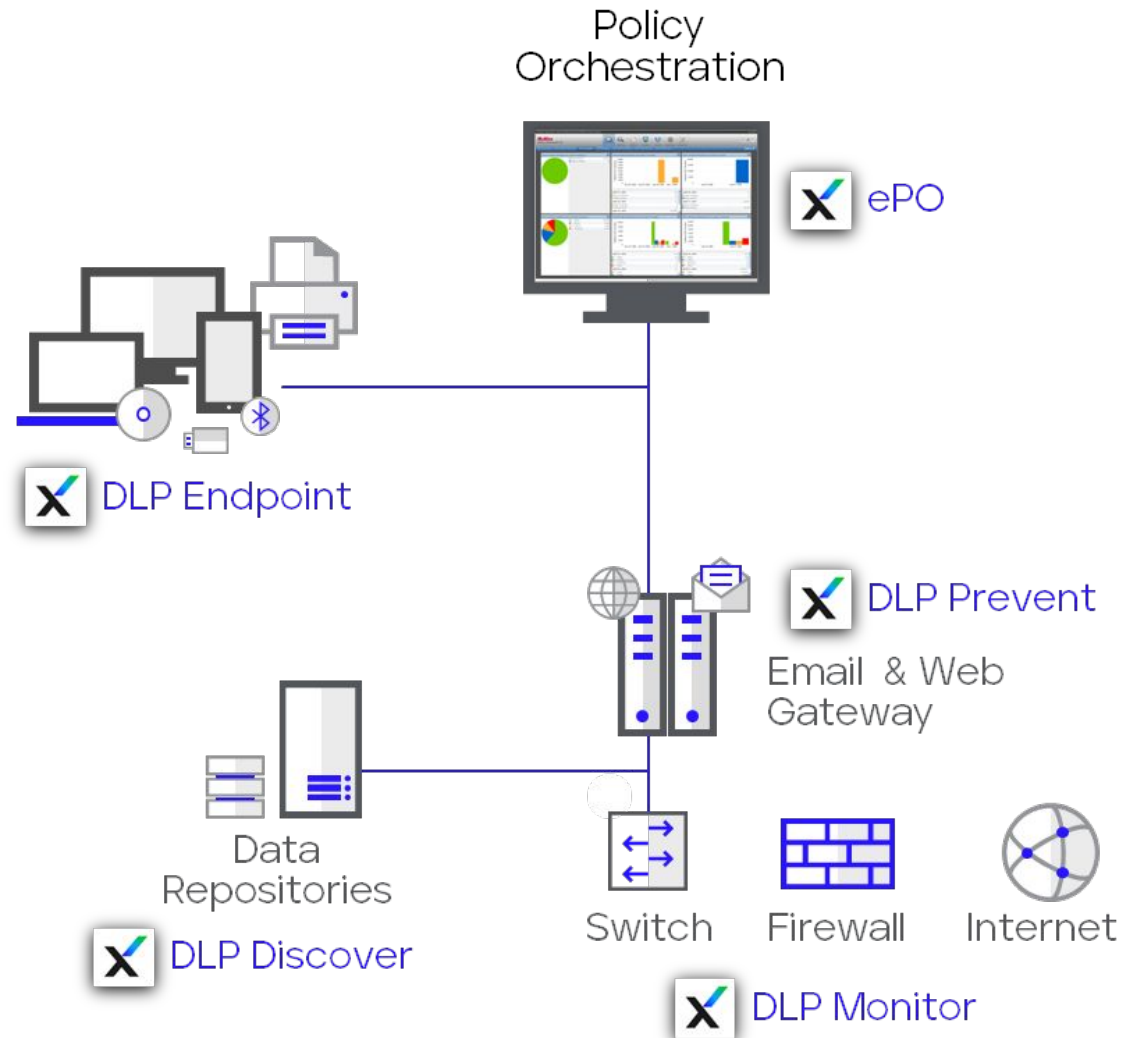
# XDR Architecture

## Trellix ENS and HX with on-prem SIEM (Air Gap)



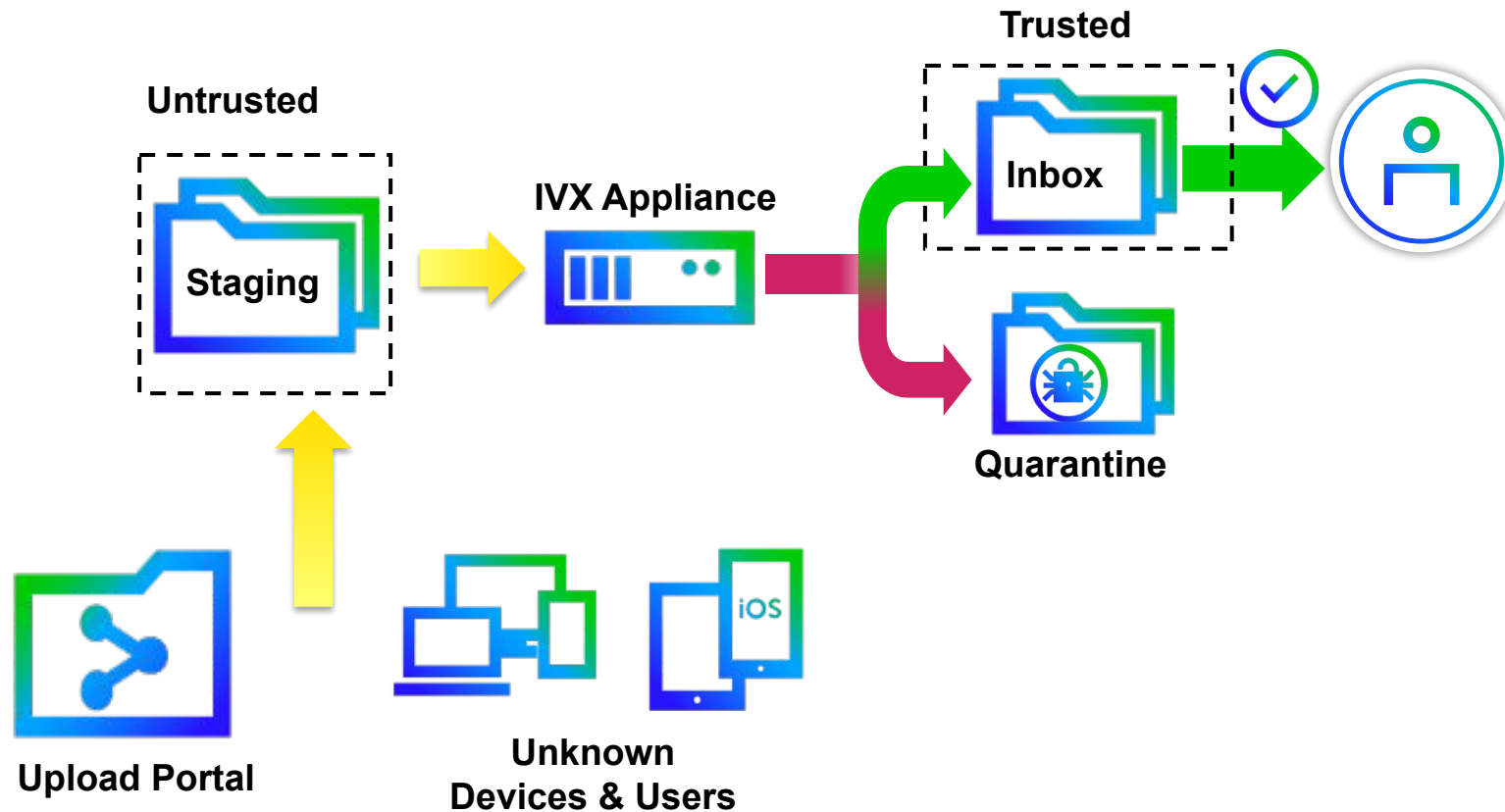
# XDR Architecture

## Data Loss Prevention



# XDR Architecture

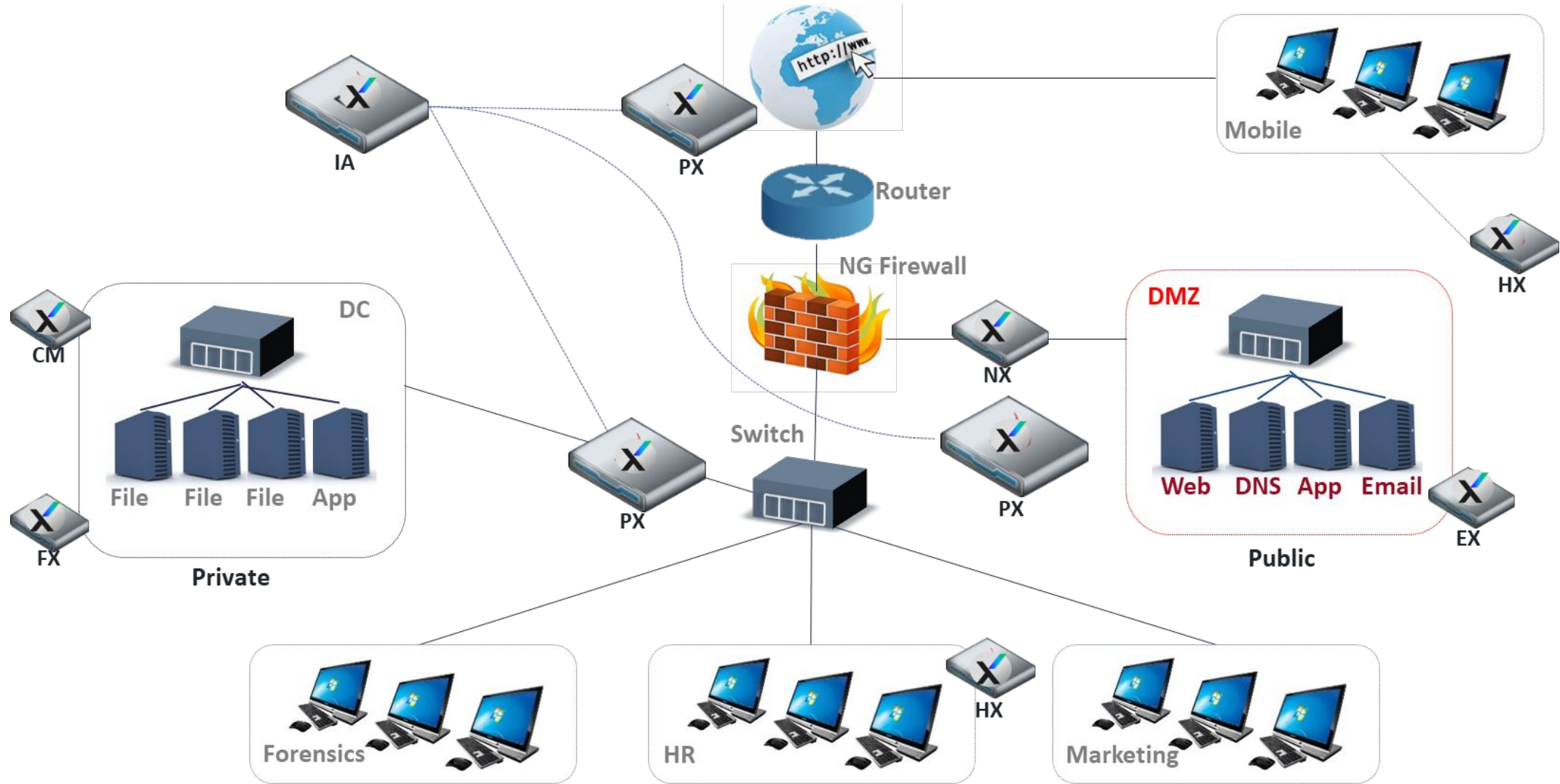
## Trusted and Untrusted File Domains



### Benefits

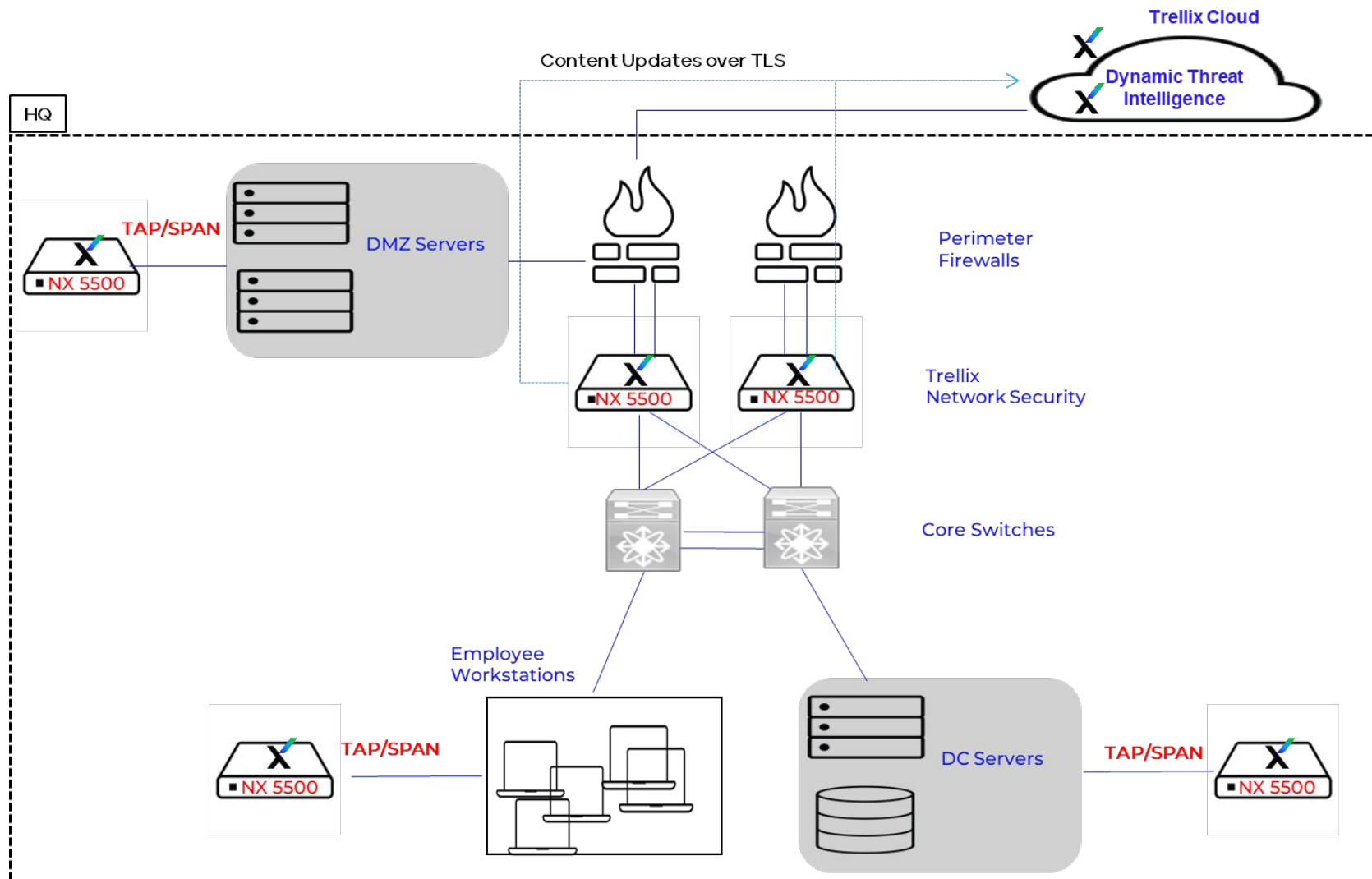
- Stop malware entering enterprise storage from untrusted area
- Ensure files are clean before end users access them

# XDR Architecture



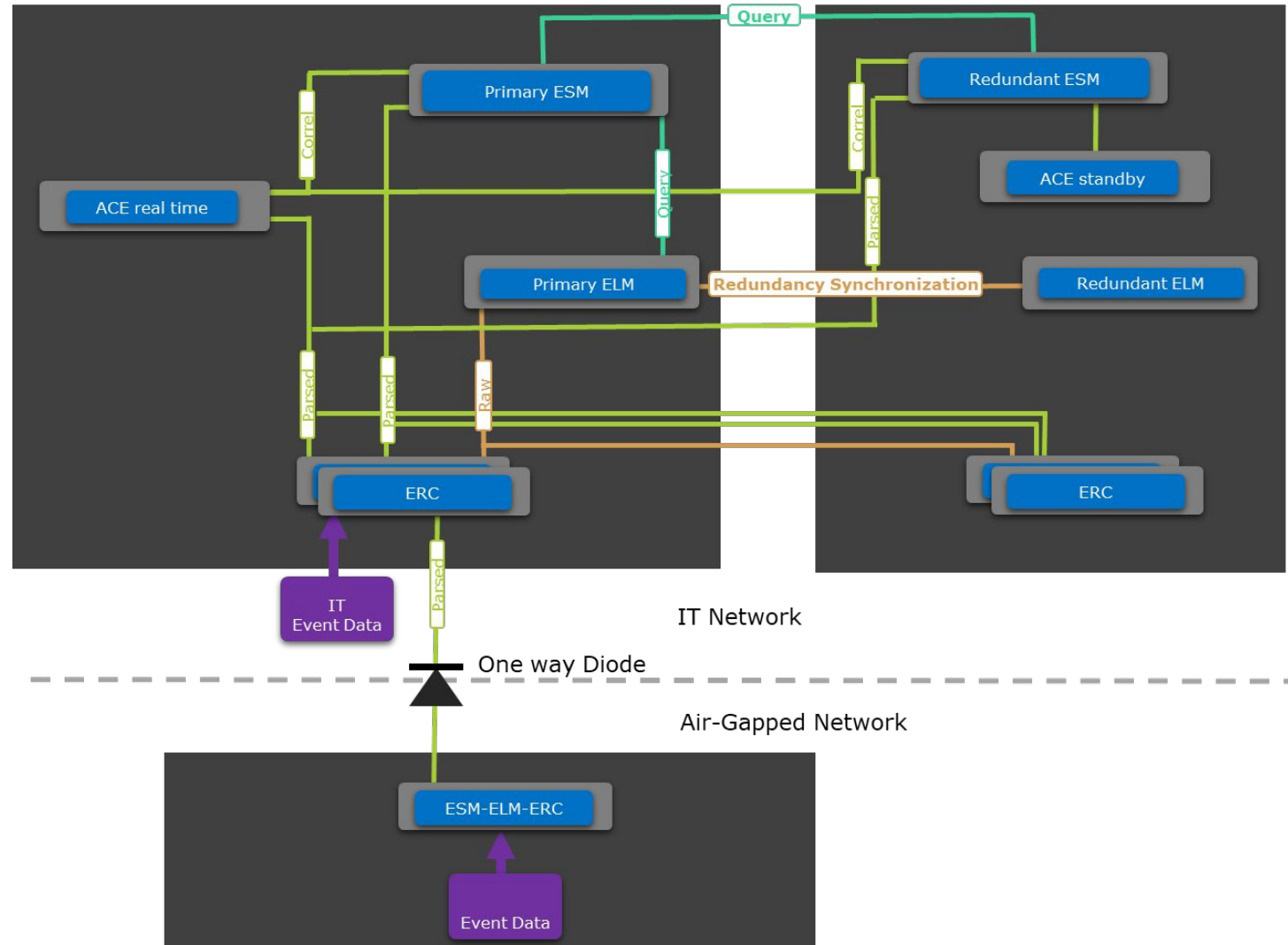


# XDR Architecture



# XDR Architecture

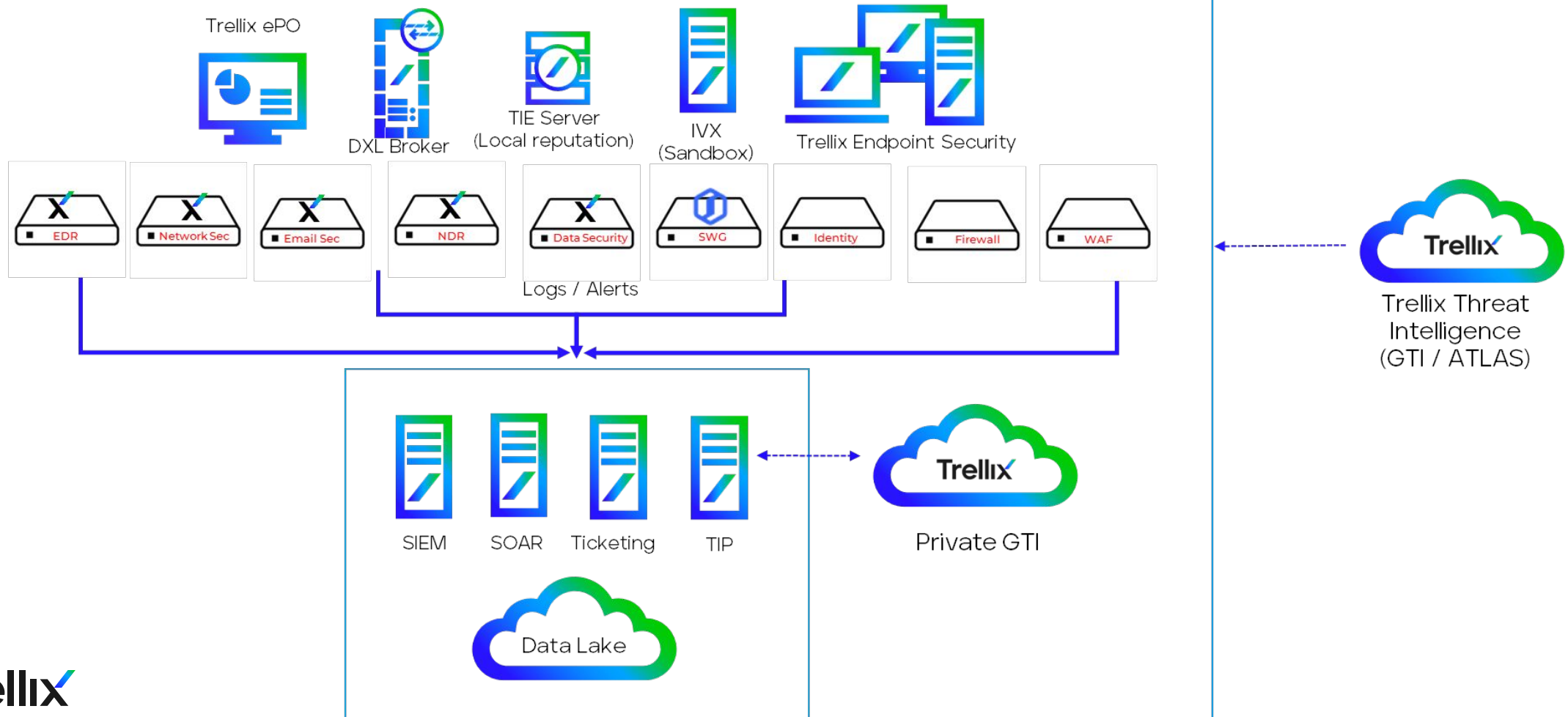
## SIEM (ESM) Architecture for Air-Gapped Networks



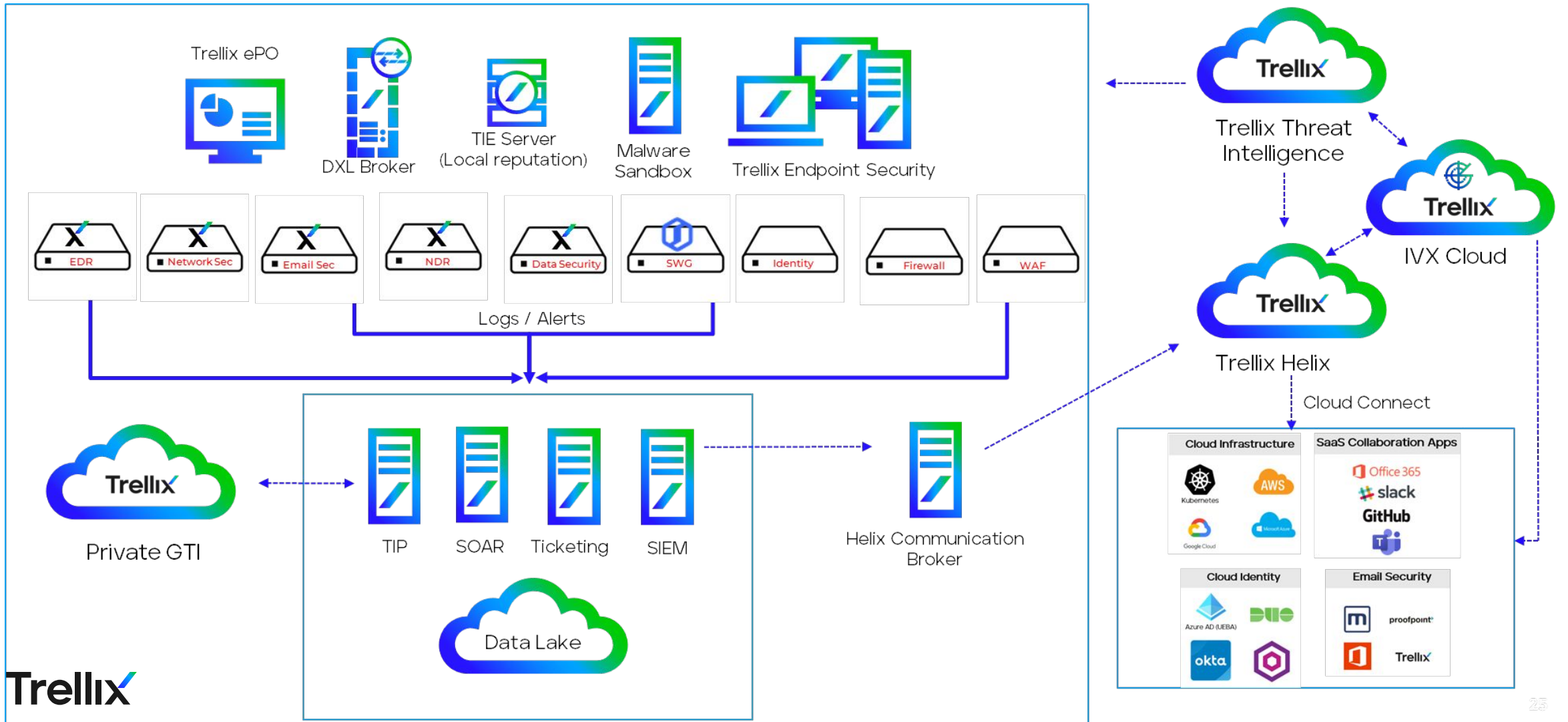
# Hybrid XDR Reference Architecture



# On-Premise XDR Architecture

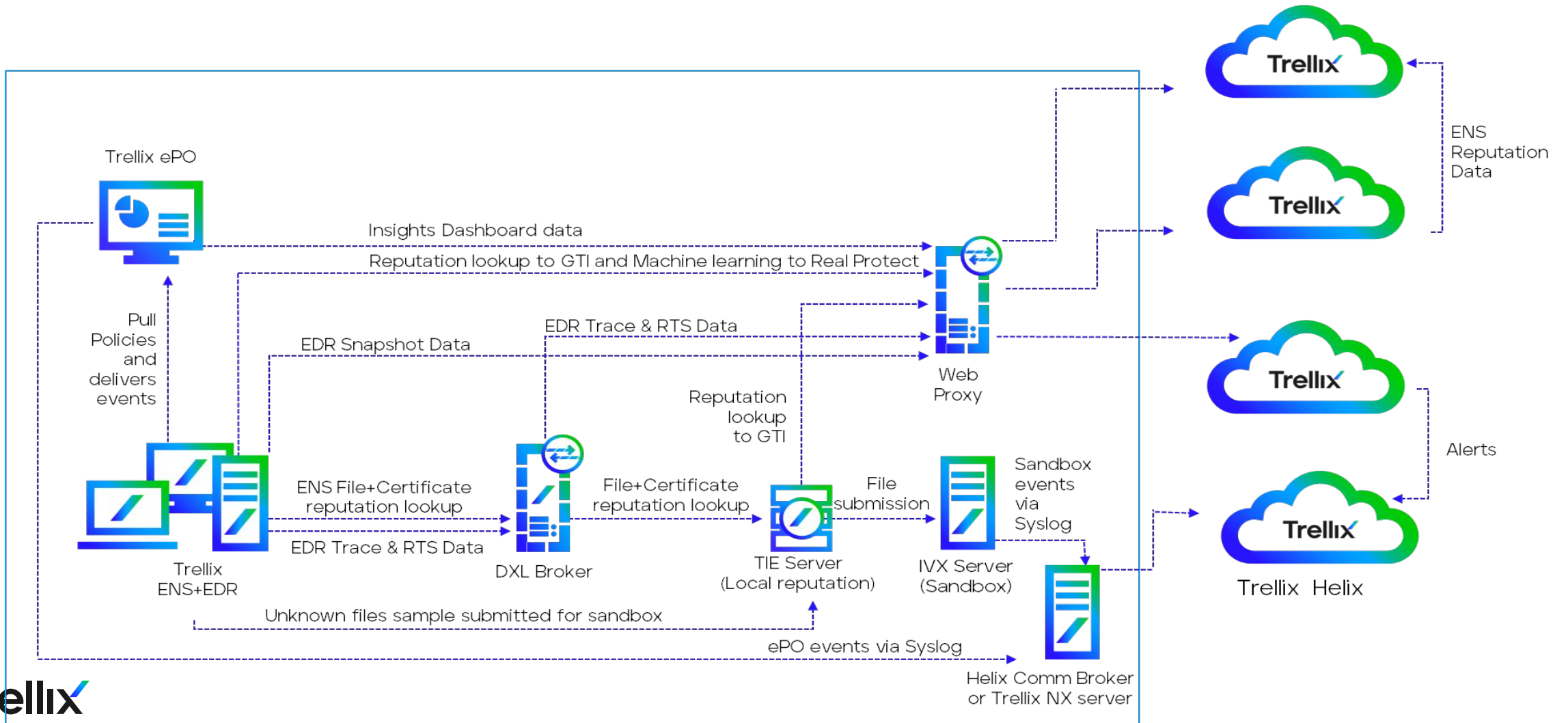


# Hybrid XDR Architecture



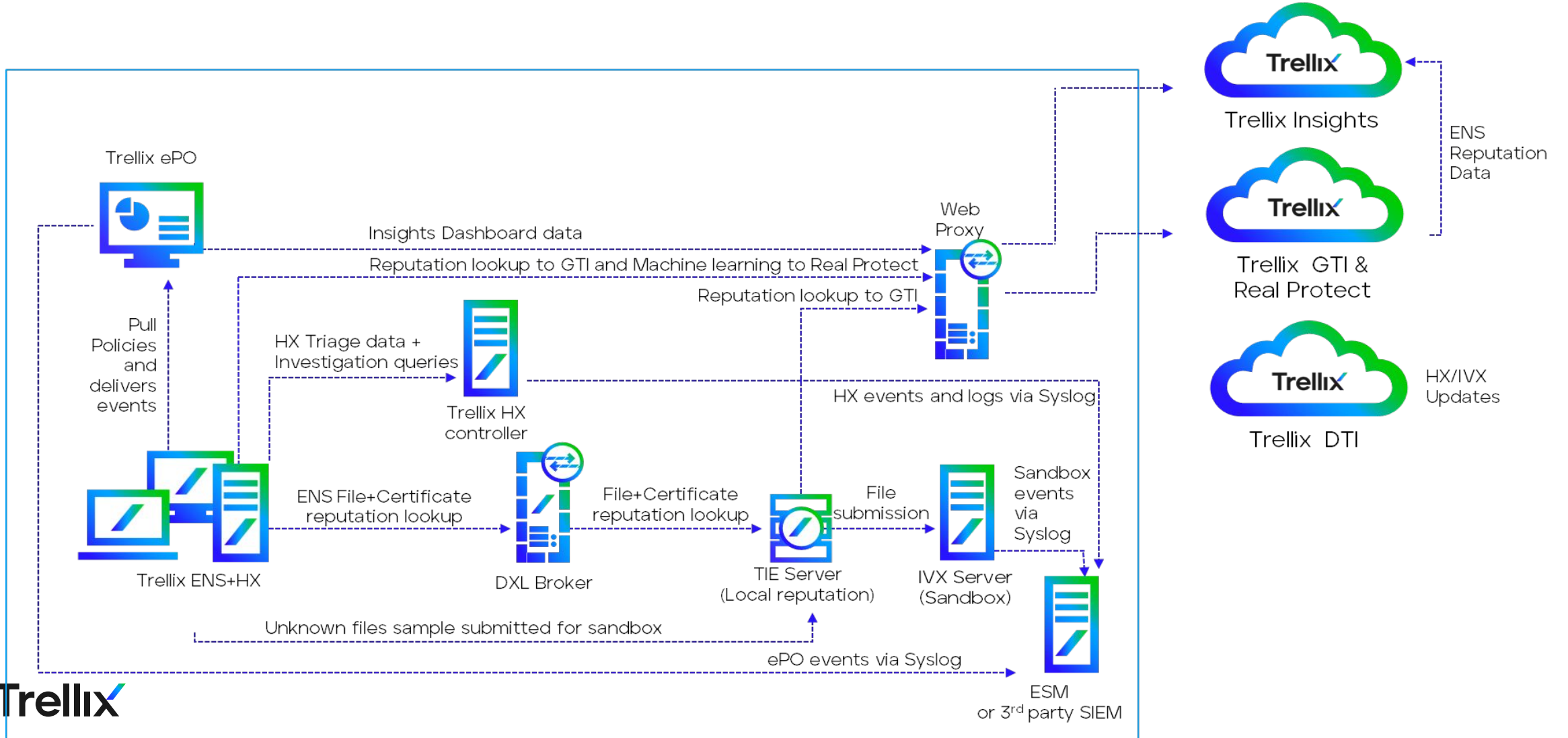
# XDR Architecture

## Trellix ENS, EDR and Helix with on-prem ePO



# XDR Architecture

## Trellix ENS and HX with on-prem SIEM





Trellix