Resilience in the Digital Age

Yakup Borekcioglu| VP of Sales, Government and BFSI in AMEA Trend Micro

An Industry Leader

$2 Billion 2022 Gross Sales†

99 Consecutive Profitable Quarters
Every quarter since going public

424,000+ SaaS Commercial Customers
500,000+ commercial customers, 175+ countries

62M+
SaaS-Protected Assets

#1 in **Cloud** Workload Security
Based on global market share*

A Leader in **XDR**
Based on offering strength and strategy**

A Leader in **EPP**
Based on completeness of vision and ability to execute***

Highest Market Share in **IDPS**
Based on sum of vendor revenue ($) for 2Q23****

#1 in Public Vulnerability Disclosure‡
+ Over **146 Billion threats blocked** in 2022

7500+ Employees in 73 Countries

*IDC Worldwide Cloud Workload Security 2022 Market Shares, #US49669822, May 2023
**The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021
‡Quantifying the Public Vulnerability Market, Omdia, May 2022

***Gartner Magic Quadrant for Endpoint Protection Platforms, 31 December 2022
****Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q23, 25 September 2023

†Constant currency

TREND MICRO™

AI Amplifying SOC Operations

New generative-AI: Plain-language interface empowering SOC analysts of varying skill level

Understand & Contextualize Alerts

Summarize events/alerts in plain-language, correlating the tactics and techniques

Develop Search Queries

Accelerate mean-time-to-contain (MTTC) by enabling SOC teams to build sophisticated search queries through plain-language interface
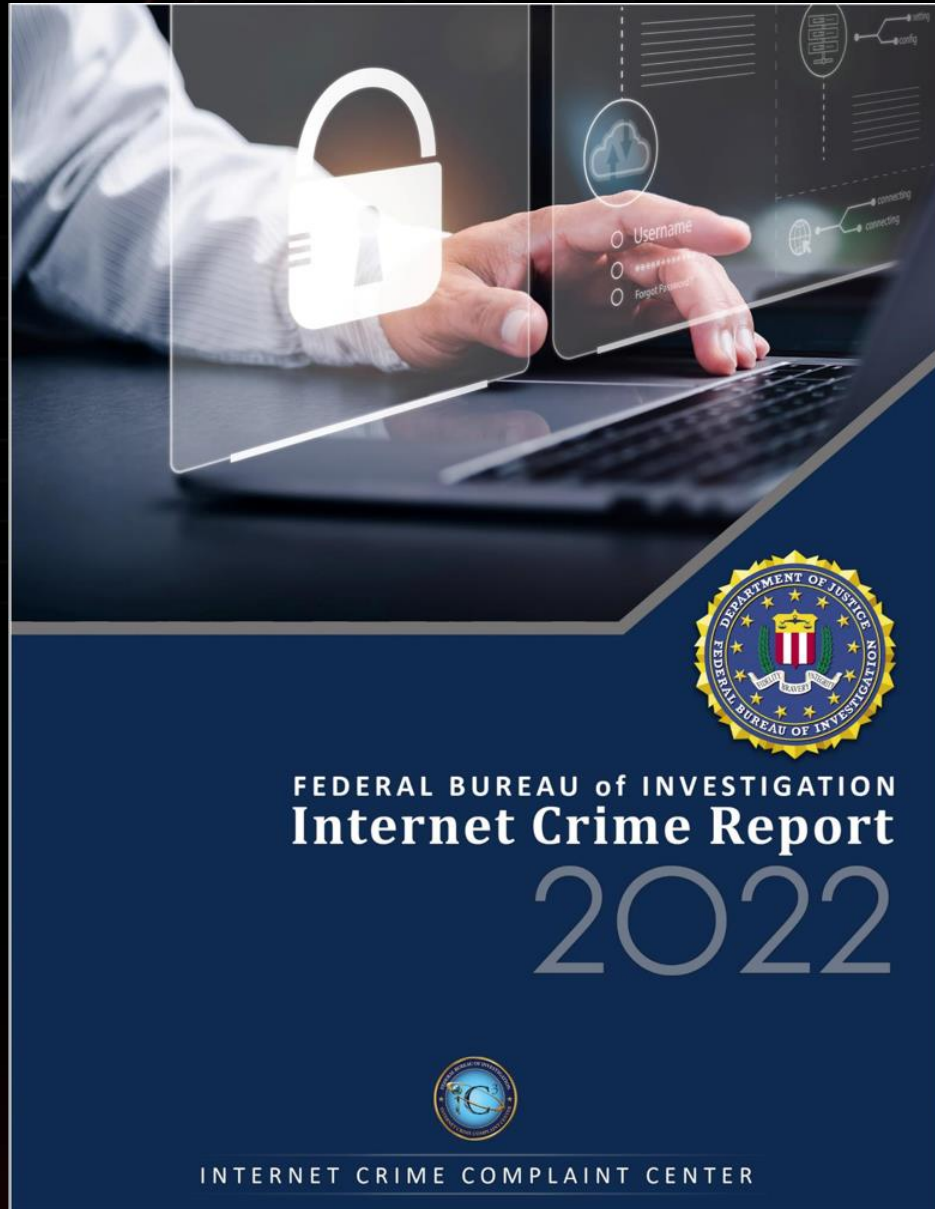
Unpack complex Scripts

Breakdown complex scripts in attacks, to quickly interpret the purpose and the intended actions, and then generate a human readable explanation

TREND MICRO™

In the hands of Cybercriminals
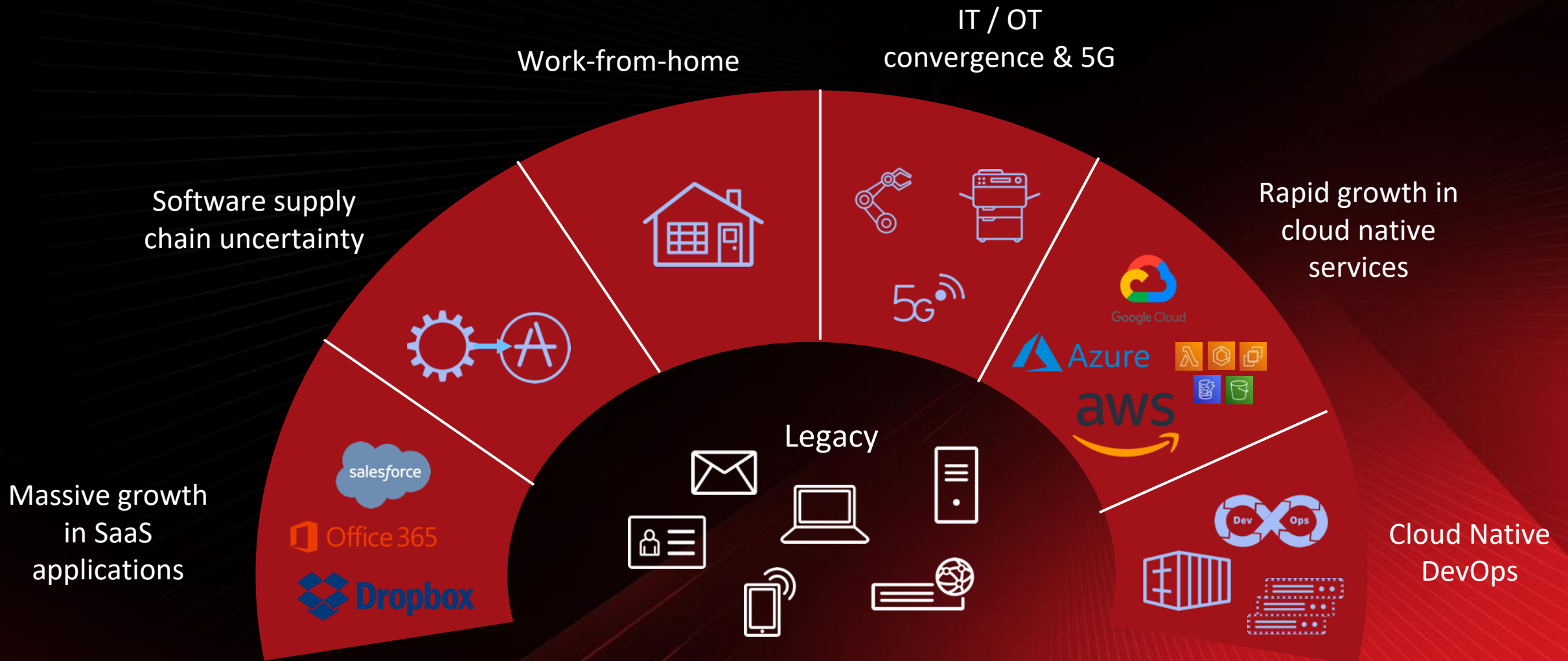
Highly Effective Social Engineering Attacks

Expanding Attack Surface

AI-Supported Password Guessing

Evasion of Security System

Sophisticated Spear Phishing Attacks

Malware Creation & Evasion

03

04

02

05

01

06

AI

TREND MICRO™

Ransomware Disruption Continues

FEDERAL BUREAU of INVESTIGATION
Internet Crime Report 2022
INTERNET CRIME COMPLAINT CENTER

By Victim Loss

Crime Type	Loss	Crime Type	Loss
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

TREND MICRO

Rising Complexity and Scale of Attack Surface

Work-from-home

IT / OT convergence & 5G

Software supply chain uncertainty

Rapid growth in cloud native services

Massive growth in SaaS applications

Legacy

Cloud Native DevOps

TREND MICRO™

Never Trust | Always Verify

Foundation of Zero Trust

Identity

Device

Network/ Environment

Application Workload

Data

Visibility and Analytics

Automation and Orchestration

Governance

User & Identity · Endpoints & Servers · Email · Network · ICS/OT · 5G · Apps · Code Repo · Cloud Infra · Data
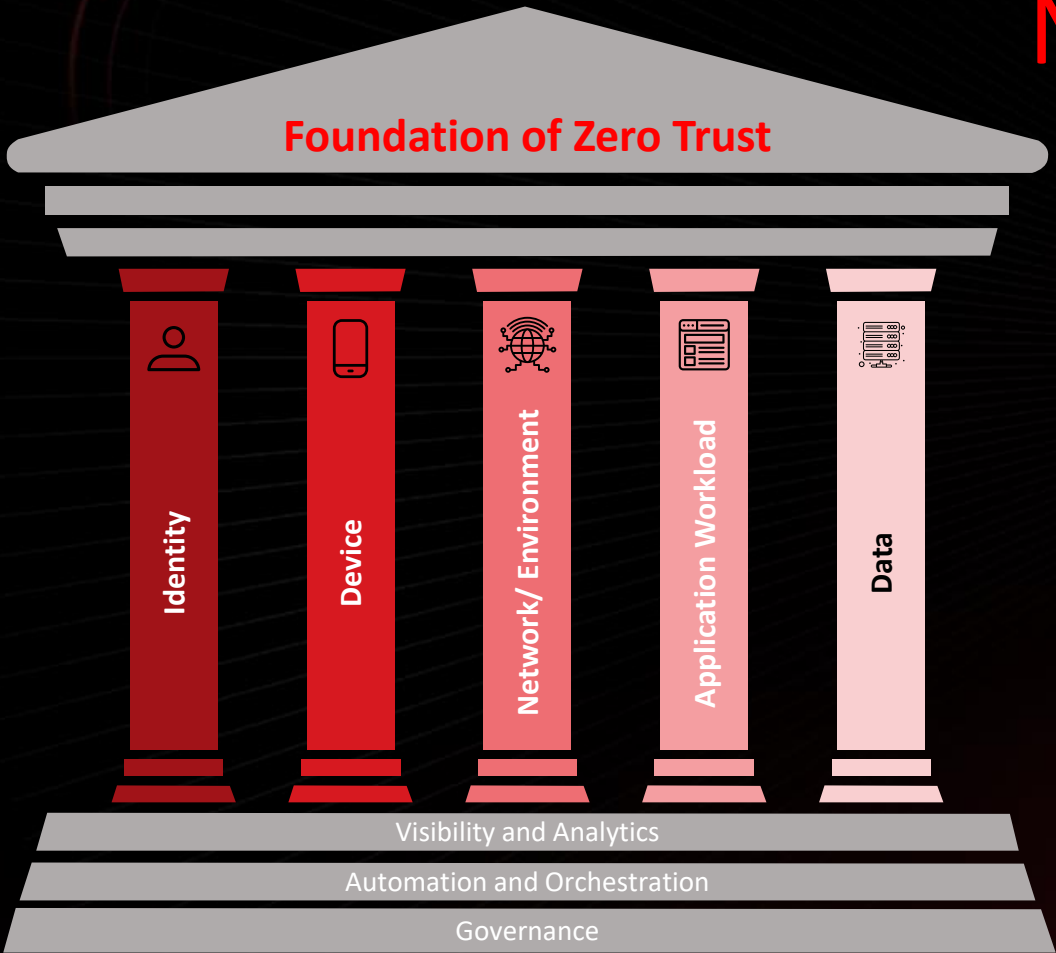
Visibility is a Foundational Need
Discovery of Attack Surface

Verify Beyond Identity
Continuously Assess Risk Scoring

Integration is Paramount
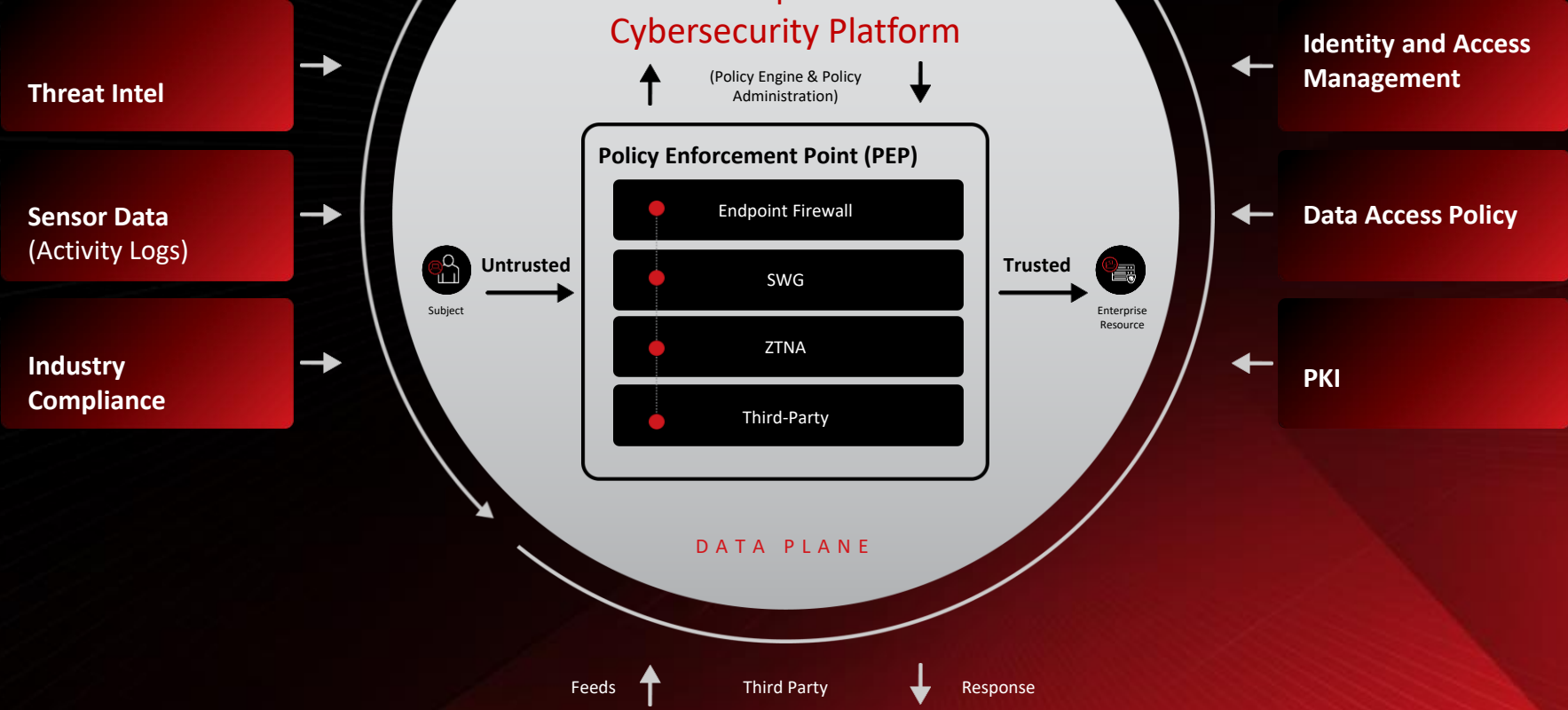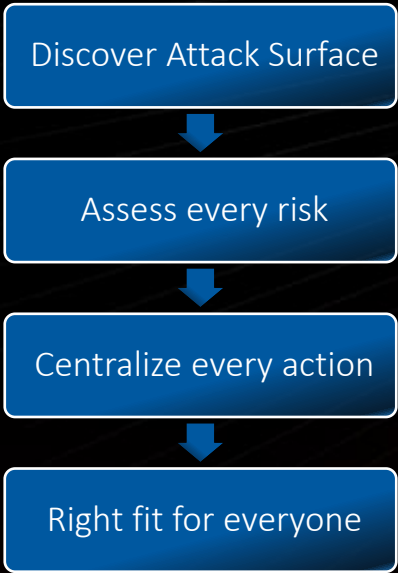Centralized Policy Decision with Native Enforcement Points

Source: United States Cybersecurity and Infrastructure Security Agency's "Zero Trust Security Model", July 2021

TREND MICRO

Native Sensors
- Identities
- Devices
- Email
- Cloud Infra
- Network
- Cloud Apps

Threat Intelligence

Third Party Integrations
Asset Information | Detection Data

Third Party Intelligence
Curated Feeds | STIX/TAXII | MISP

Risk-based | AI Powered Cybersecurity Platform

XDR

Discover Attack Surface

Risk-based Cybersecurity Platform

Mitigate Risk

Assess Risk

XDR

XDR

CONTINUOUS ASSESSMENTS

POLICY MANAGEMENT

Risk Scoring
- Identities 88
- Devices 15
- Cloud Apps 52

Zero Trust Secure Access
- Zero Trust Network Access
- Secure Web Gateway

Native Enforcement Points
- Network
- Devices
- Cloud Apps
- Email

Third Party Integrations
PEP | SOAR | Web Hook | API

TREND MICRO

Platform Approach to Cybersecurity

Accelerating Security & Business Outcomes

Modernizing Cybersecurity

Improve cyber security outcomes through platform consolidation

From Risk to Resilience

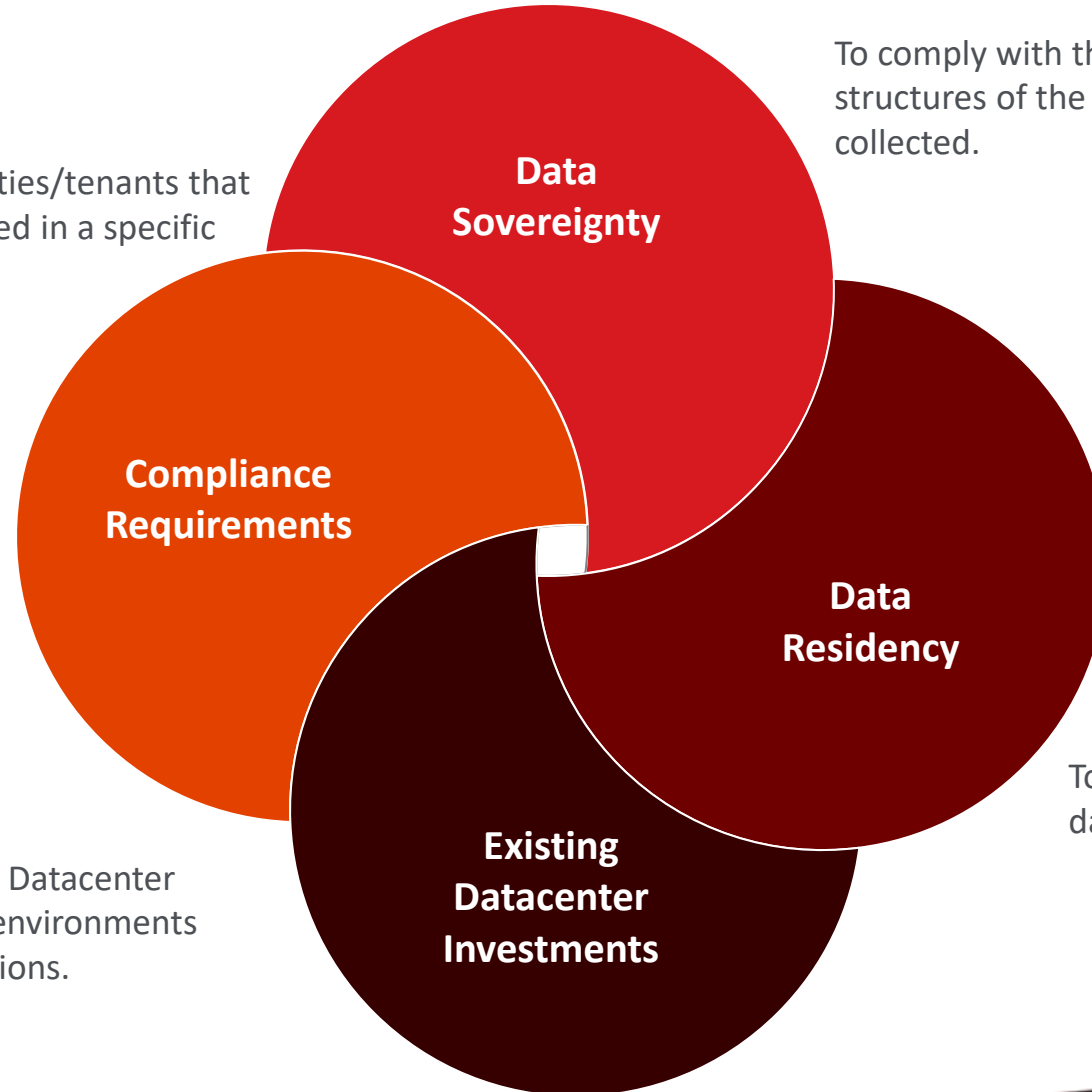Proactively discover attack surface, assess and mitigate (reduce) cyber risks

Operationalize Zero Trust

No matter where you are in your Zero Trust journey

TREND MICRO™

The need for an XDR on-premise

Compliance agreements with entities/tenants that require data to be stored/processed in a specific location.

To comply with the laws and governance structures of the nation where the data is collected.

Data Sovereignty

Compliance Requirements

Data Residency

Existing Datacenter Investments

Take advantage of the existing Datacenter Investments, and to adapt to environments with network/internet restrictions.

To comply with data localization of regulated data within a particular region or country.

TREND MICRO™

Trend Micro One Box - Architecture

Components Hosted in TM One Box

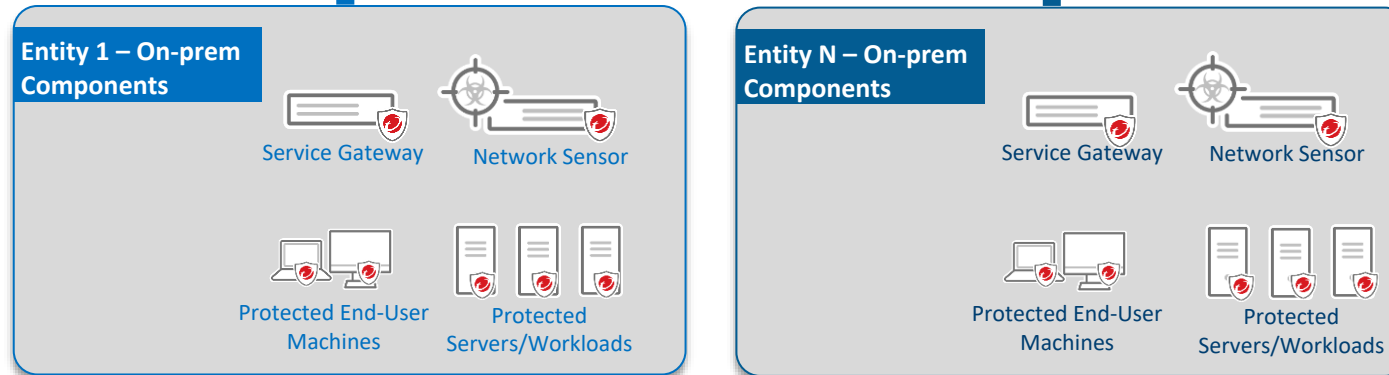**Central SOC Console**
Visibility, Detection & Response, Threat Intelligence sharing across all Entities

Govt./MSP Datacenter

Entity 1 – XDR, EPP Instances
- XDR
- EPP
- Sandbox

Entity N.. – XDR, EPP Instances
- XDR
- EPP
- Sandbox
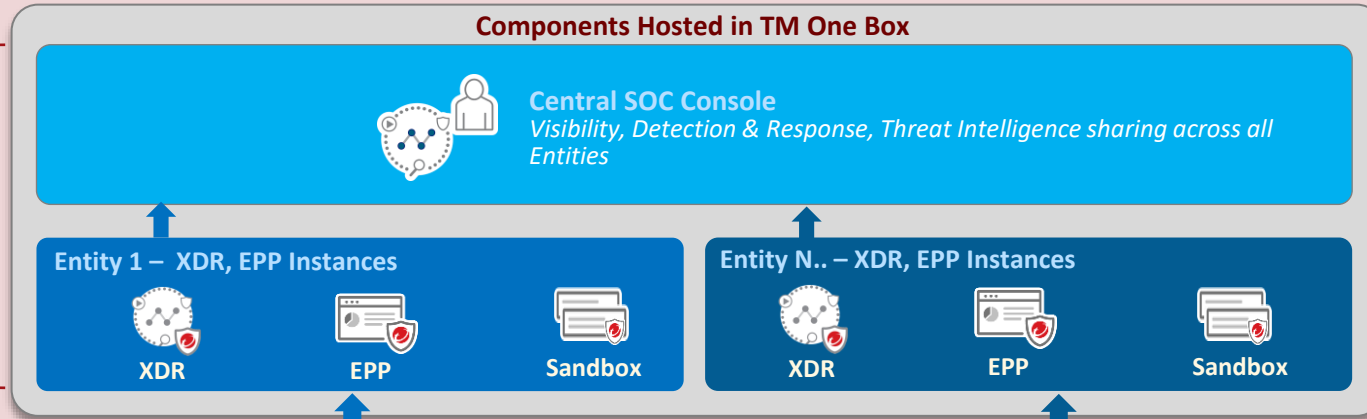
Provides **advanced threat hunting, detection, and response** to Entities that seek **assistance** for their own incident response staff.

Dedicated XDR, EPP Instances per Entity. Each entity has a dedicated and independent environment.

Entity 1 – On-prem Components
- Service Gateway
- Network Sensor
- Protected End-User Machines
- Protected Servers/Workloads

Entity N – On-prem Components
- Service Gateway
- Network Sensor
- Protected End-User Machines
- Protected Servers/Workloads

Solutions deployed across the Entity IT environment **provide protection** against threats and **work as a Sensors** for the XDR platform

Components Deployed in Entity/Tenant Environment

TREND MICRO™

Trend Micro One Box gives you...

03 Supports Air-gapped environments

04 Designed for Multi-tenant

02 Solves data sovereignty & residency challenges

05 Central visibility across multiple entities/tenants

01 Purpose built on-premise XDR solution

06 Sizing options to fit different environments

TREND MICRO SMART Protection Network
Threat Intelligence

Trend Micro One Box

TREND MICRO