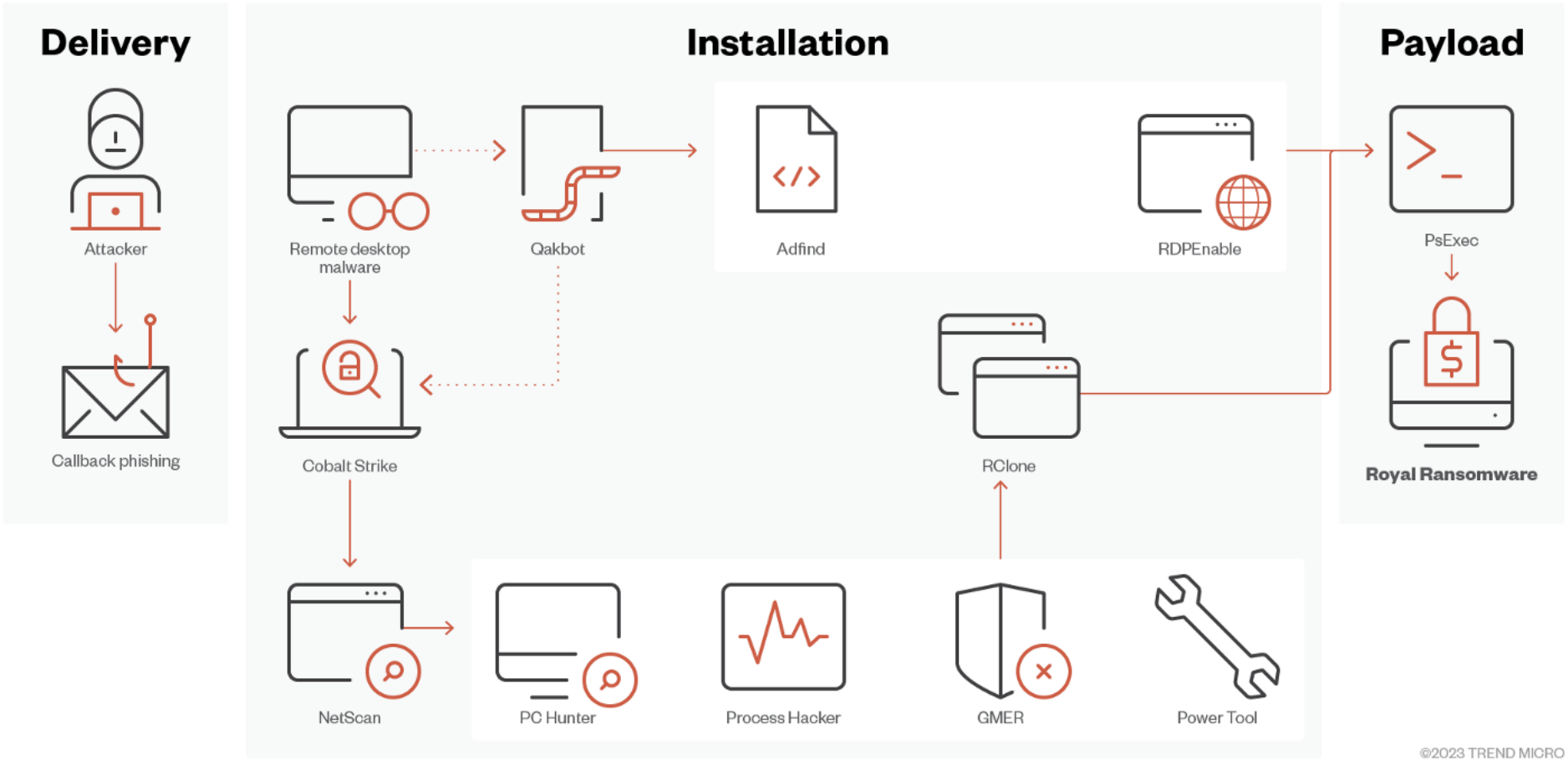
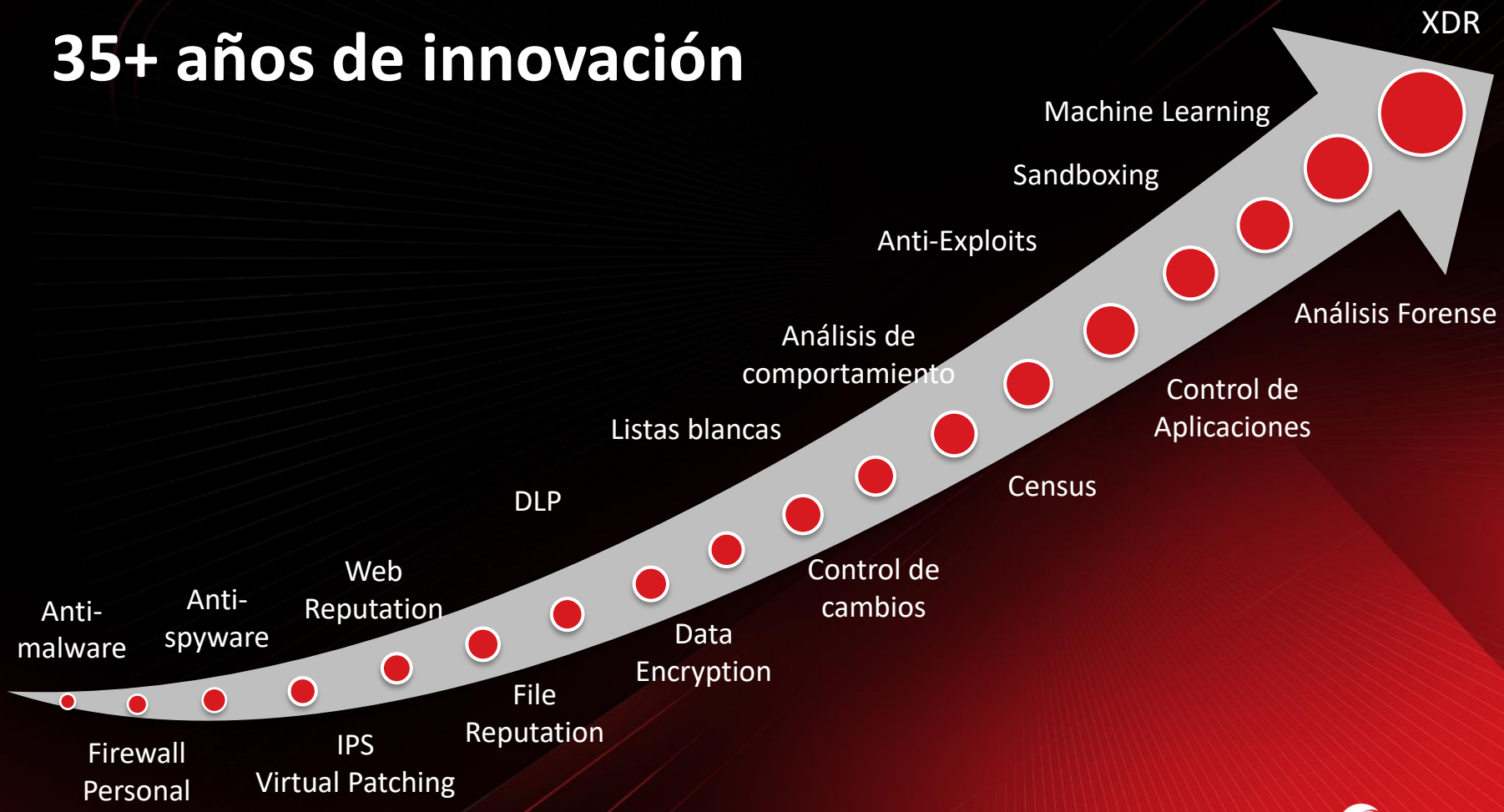
El ABC de la Cyberseguridad

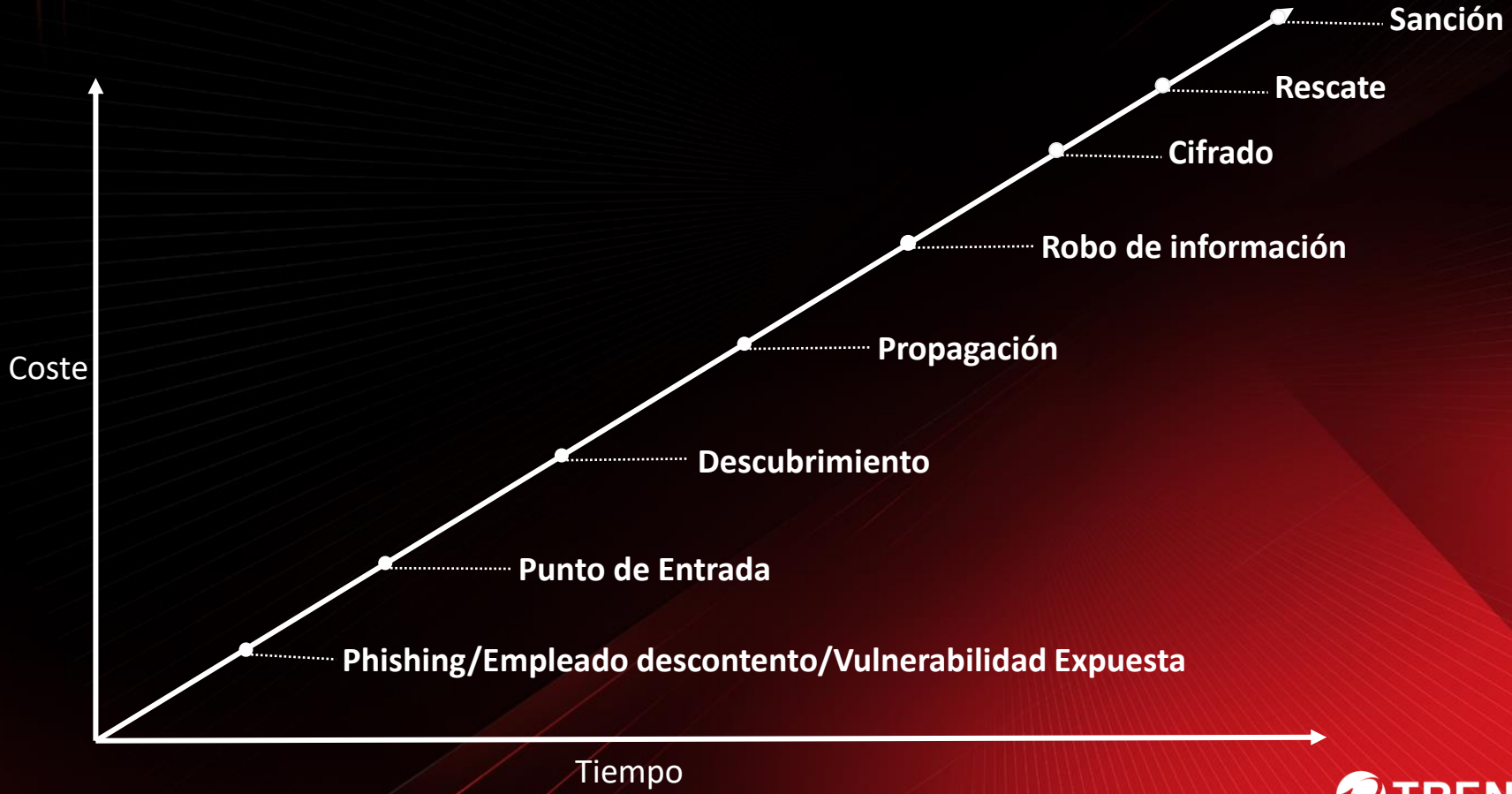
Jesús Gayoso Cuesta
Sales Engineer.



35+ años de innovación



Coste = Cómo x Cuándo



TREND MICRO Vision One

Cybersecurity Platform

Análisis de la postura de seguridad.

Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)


User and Identity


Email


Endpoints and Servers


Cloud Infrastructure


Applications


Code Repository


Data


Network

5G


ICS/OT

Email Security | **Endpoint** Security | **Cloud** Security | **Network** Security | **Data** Security | **Identity** Security

Risk Mitigation • IT Automation — **Orchestration and Automation** — Custom Playbooks • Case Management

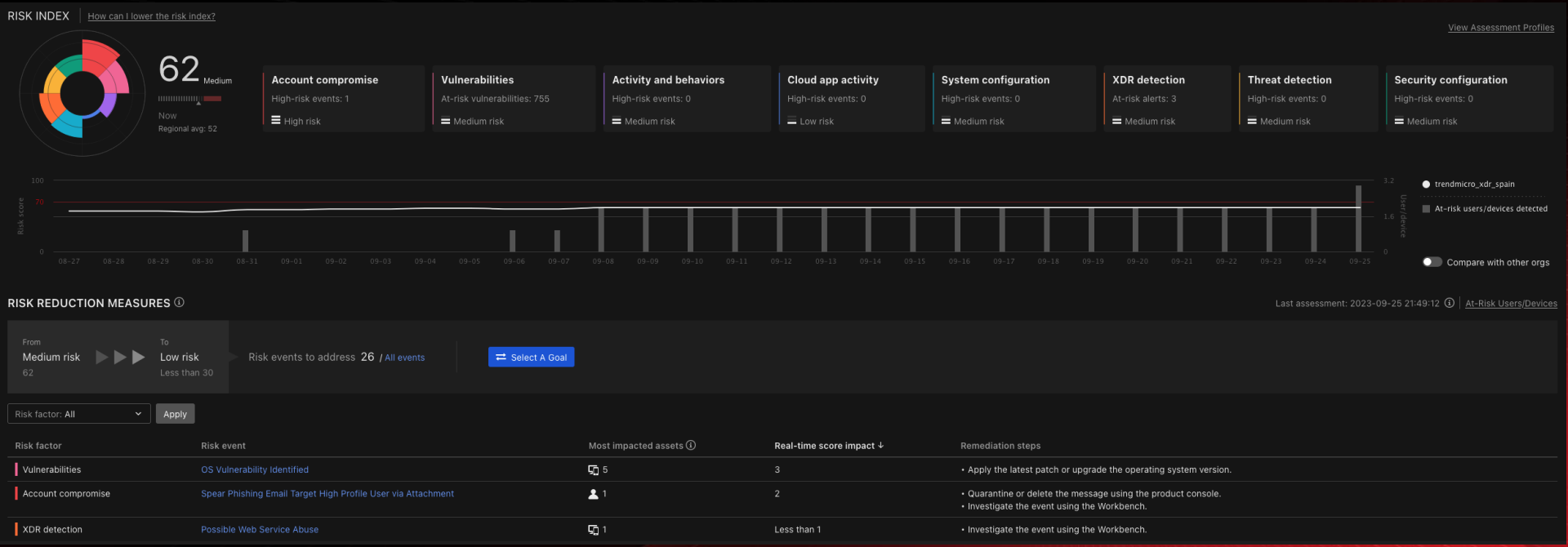
Attack Surface Intelligence • Zero Day Initiative — **Global Threat Intelligence** — Threat Research • Big Data Analytics

AI Privacy and Ethics • AI Companion — **AI Native Foundation** — Generative AI • Custom LLM • Machine Learning

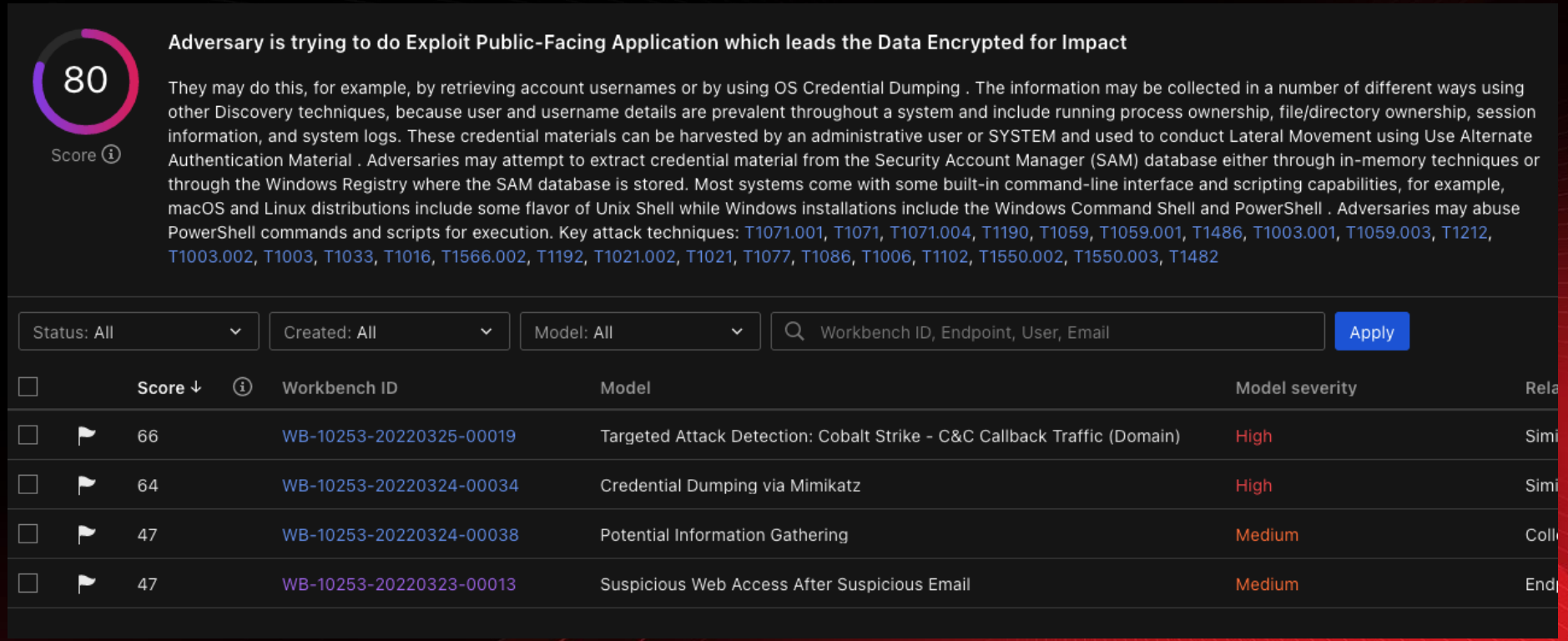
Managed Services

Ecosystem Integration

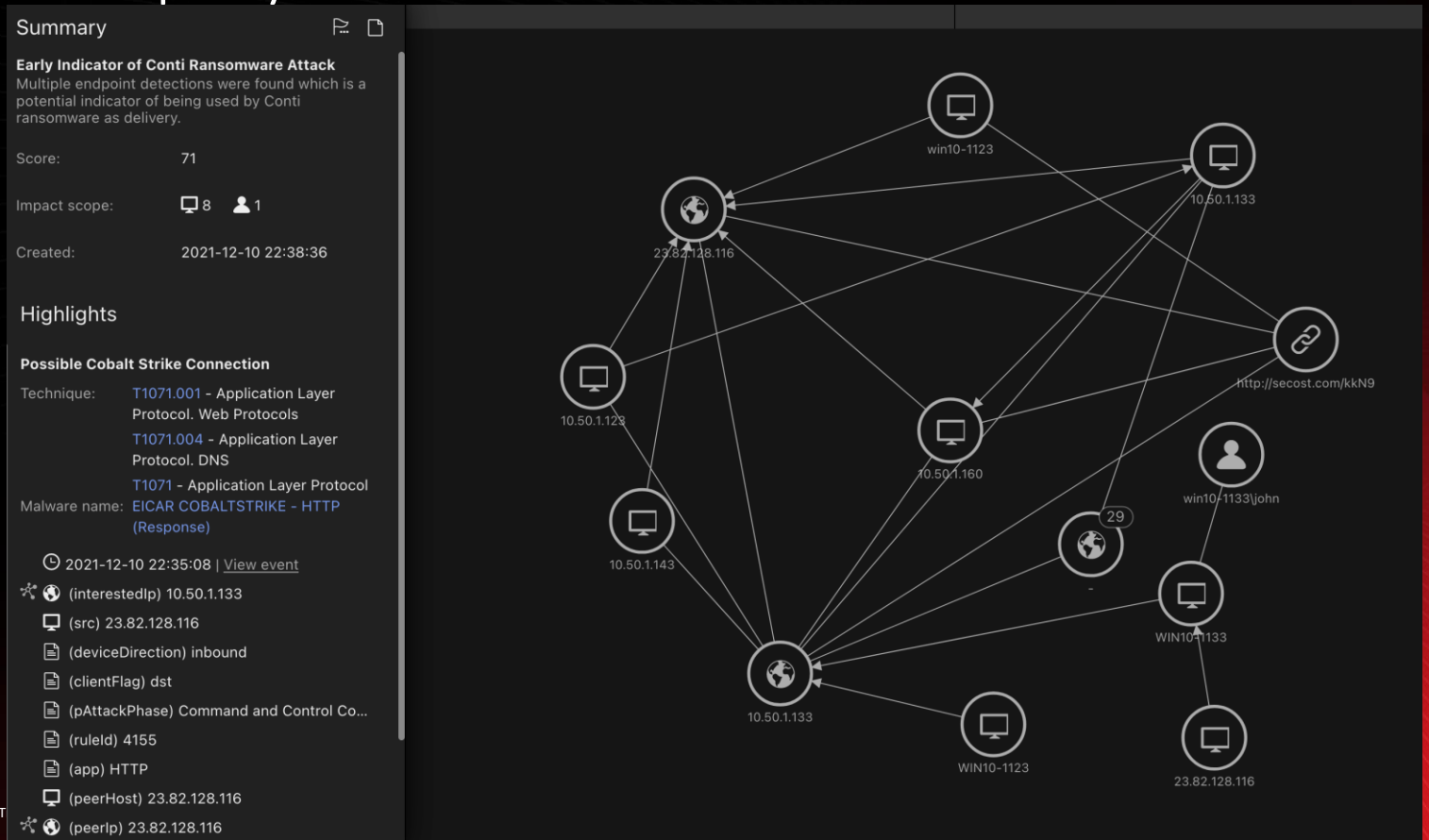
Análisis de la postura de Seguridad.



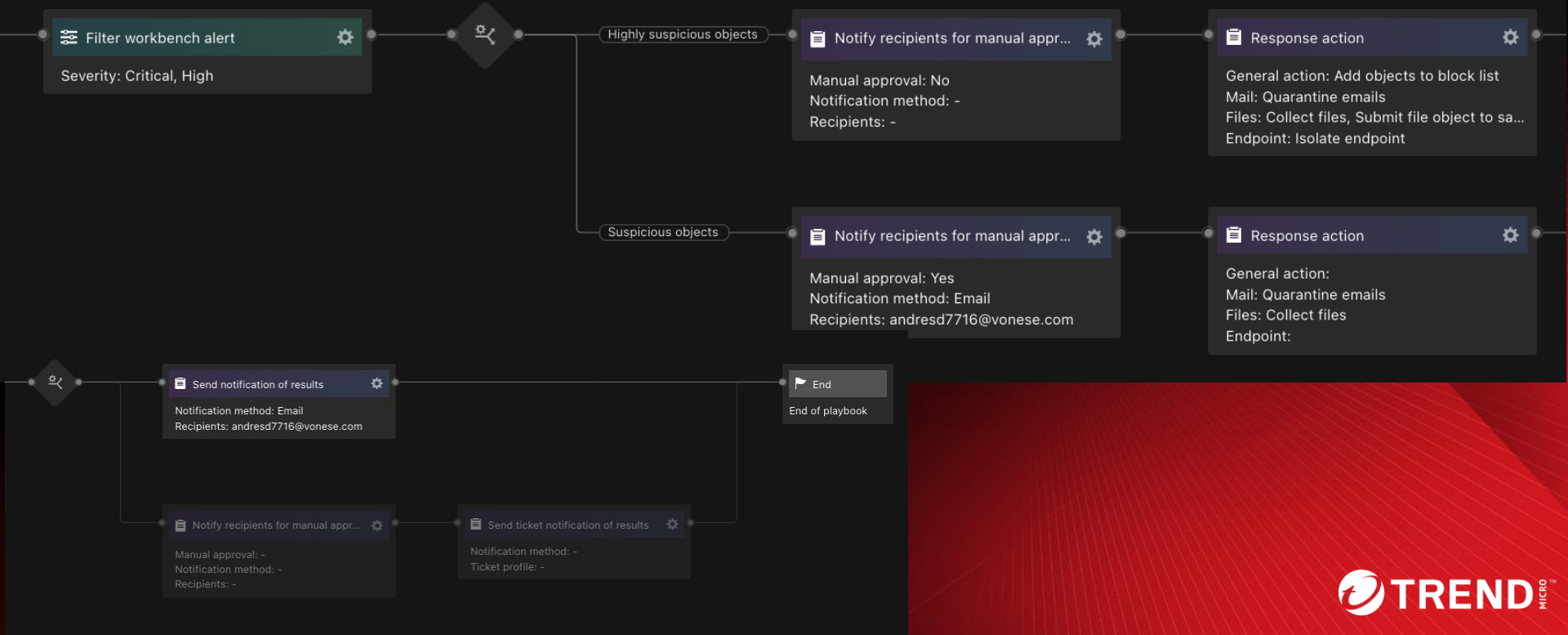
Bloqueo y detección del incidente.



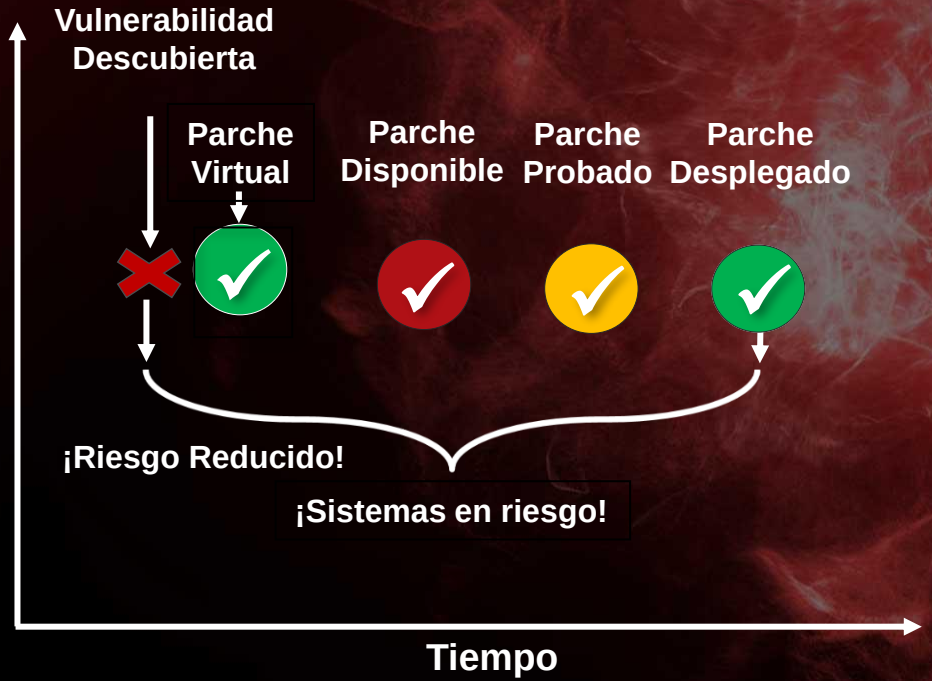
Bloqueo y detección del incidente.



Control y respuesta.

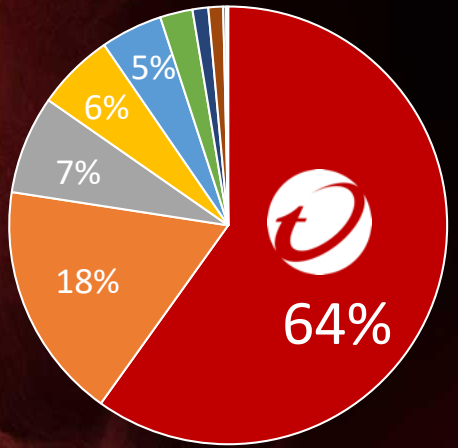


Virtual Patching



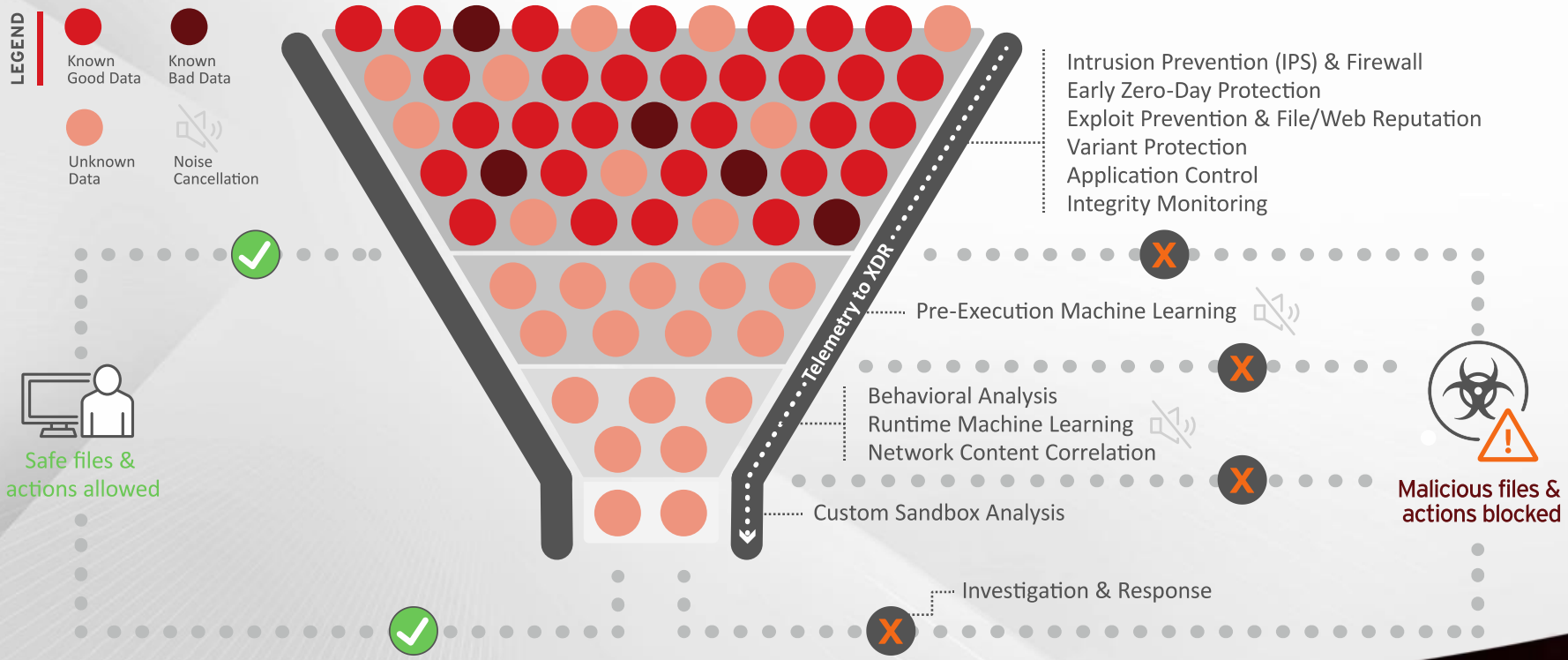
Más de 300 aplicaciones protegidas
Sistemas Operativos
BBDD
Servidores Web
Servidores de Correo
Servidores Aplicaciones
Servidores de Backup
Servidores de gestión
Servidores DHCP,FTP, etc
Aplicaciones de escritorio
Clientes de correo
Navegadores Web
Antivirus
Etc…

ZERO DAY INITIATIVE



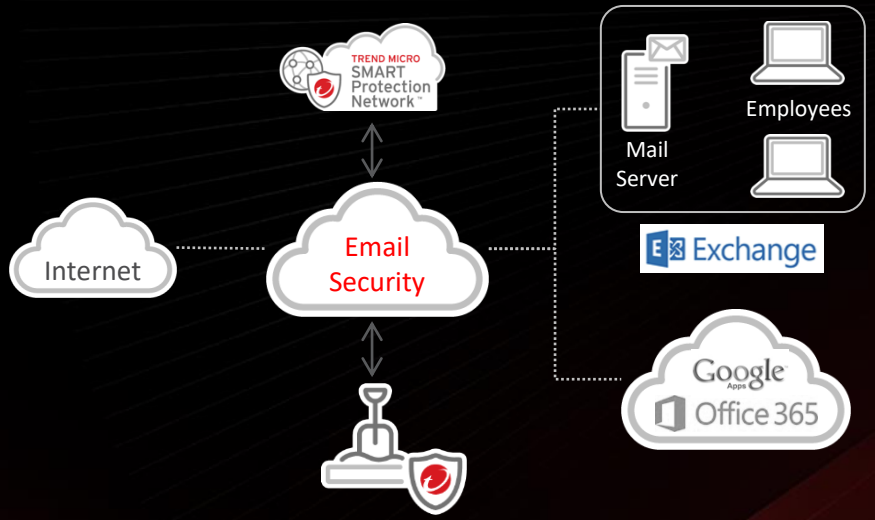
Incluido soporte para SO descontinuados por fabricante (Win 2000,2003,2008, XP,7, Ubuntu 10.04, RHEL etc)

A Platform Approach to Layered Security

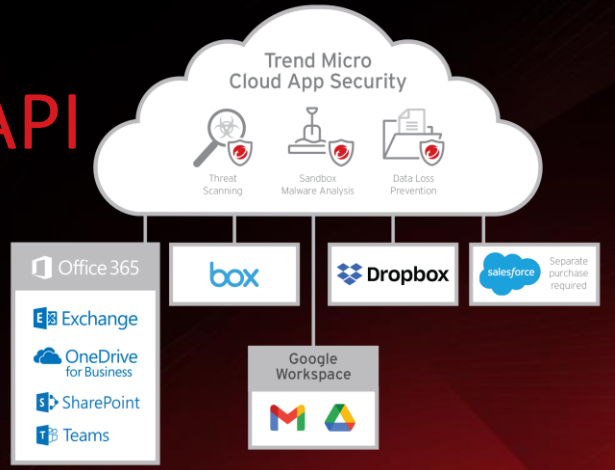


Protección de correo y telemetría

MTA

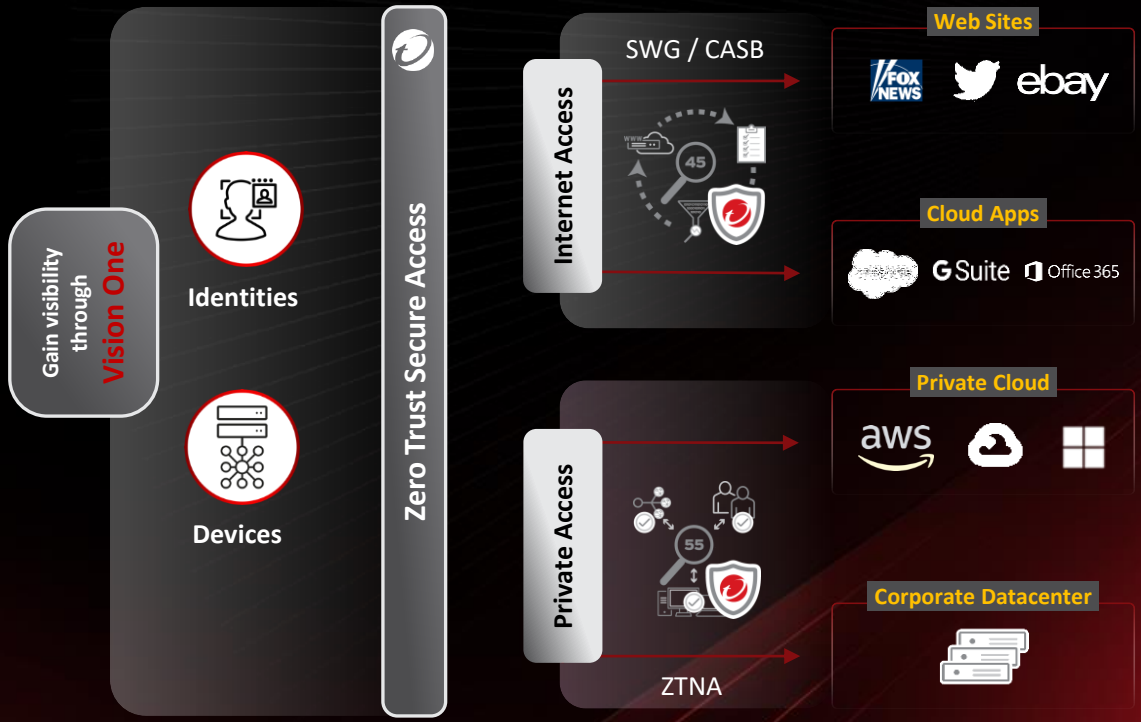


API



Email Sensor

Zero Trust Secure Access - Secure Service Edge



Evolución del proxy.
Gestión de riesgos y aplicación de politicas dinamicas en base al riesgo.

Acceso privado para aplicaciones sin publicar VPN

Misma experiencia de usuario ya sea en la oficina o de forma remota.

Combinando reglas de acceso estáticas y dinámicas

Full Stack of Control

User / Group Specific

Application Specific

Time Control

Geolocation

Device Posture

Risk Score

Acceptable

El usuario o dispositivo esta en riesgo?

Risky

Acceso denegado

And

Bloqueo de la cuenta del usuario

Access Policy

All Accounting Users

CRM Application

Only when in the office

During business hours

If AV and EDR are installed and up to date.

Only if user & device risk are low

Grant Access

Detección y respuesta

Summary

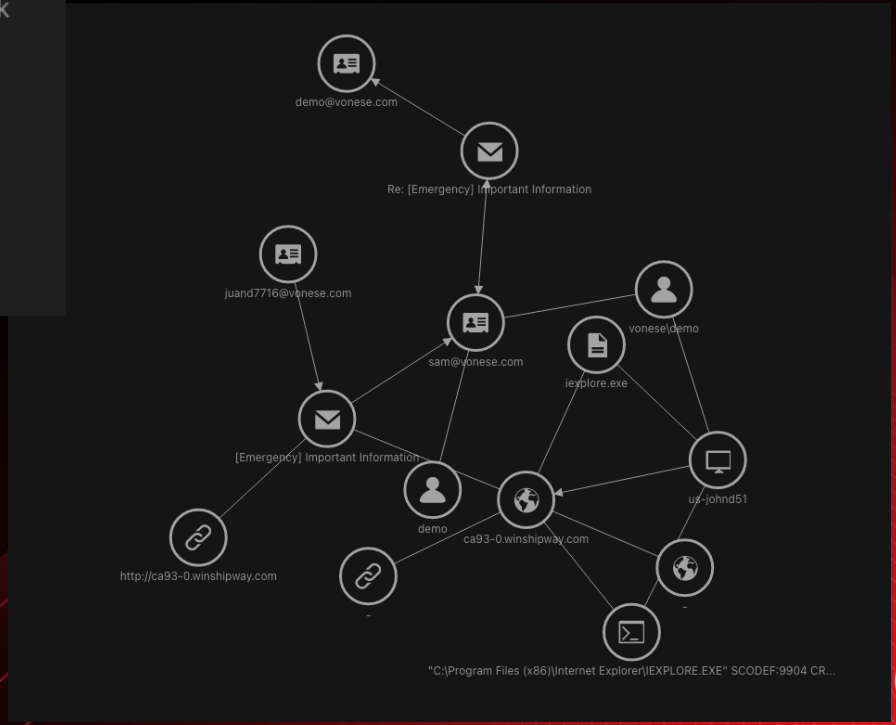
Suspicious Web Access After Suspicious Email

A user has accessed a possible spearphishing link embedded in an email message.

Score: 47

Impact scope: 1 2 3

Created: 2022-03-23 15:55:38

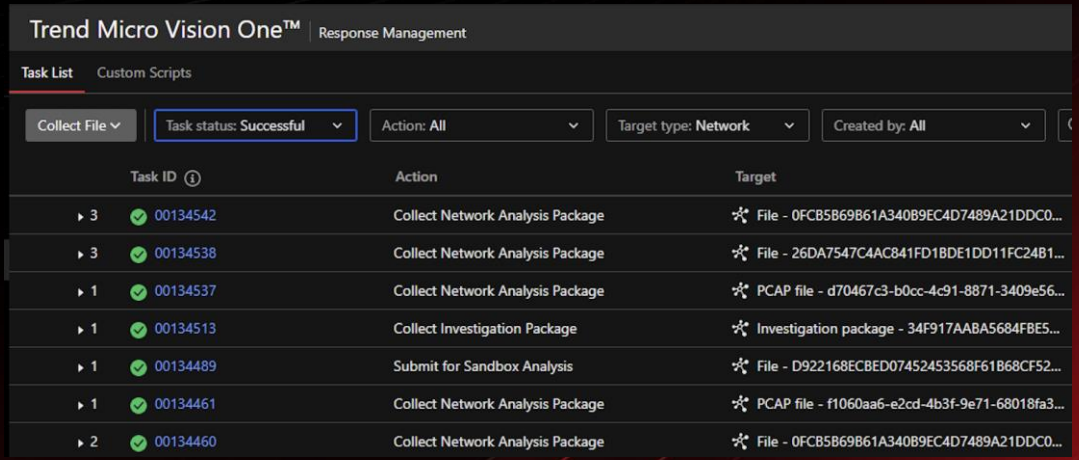


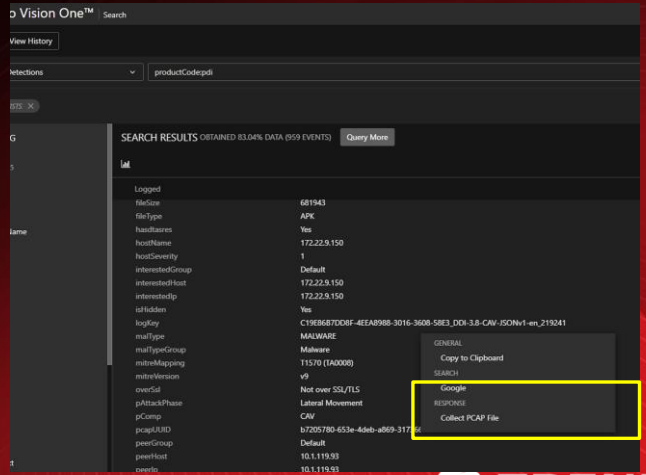
XDR – Acciones de respuesta

Type	Field Name	Response Actions	
File	fileHash	* Submit to Sandbox	* Add to Block list
Host	EndpointGuid PeerEndpointGuid	* Isolate Endpoint * Run Custom Script	* Remote Shell * Run TMIK
UserAccount	sUser1/dUser1 domainName+suid	* Disable/Enable User Account * Force Password Reset	* Force Sign out * Lock Account
Domain	hostName	* Add to Block List	
IP	src/dst/interestedIp/peerIp	* Add to Block List	
URL	request	* Submit URL to Sandbox	* Add to Block List
Email	msgId	* Quarantine message	* Delete message
EmailAccount	suser	* Add to Block list	

XDR – Acciones de respuesta – Network.

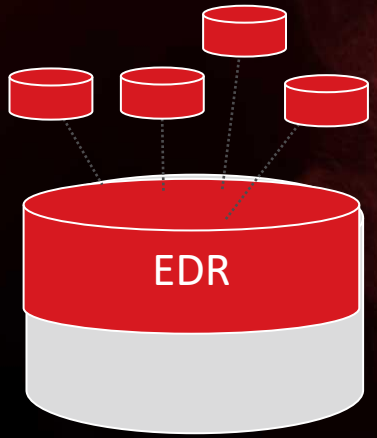
Response Action	How to trigger action	Search	OAT	WB
Collect file	field (fileHash)	Yes	Yes	Yes
Collect Investigation Package	field (fileHash)	Yes	Yes	Yes
Collect PCAP File	field (pcapUUID)	Yes	Yes	-
Collect Network Analysis Package (containing above files if any)	event	Yes	Yes	Yes





Diferentes enfoques de XDR en el Mercado

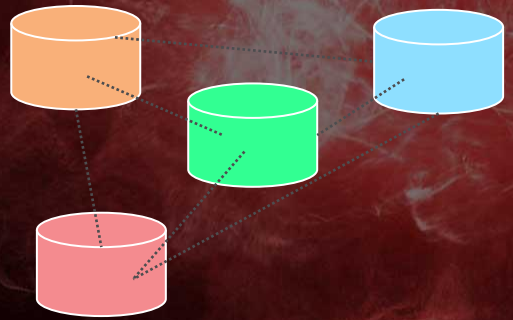
Extended EDR



Foco en el Endpoint

- Telemetría y detecciones recogidas del endpoint.

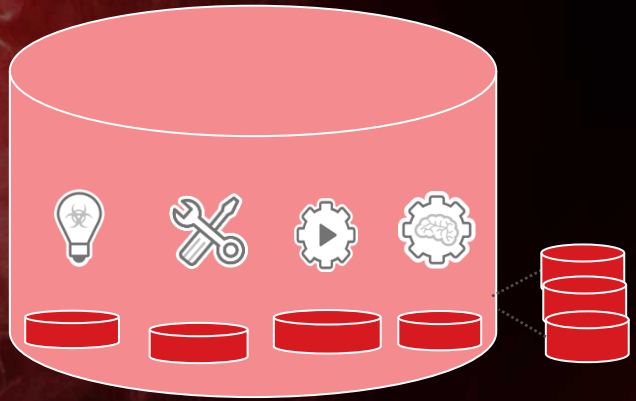
XDR Con Alianzas



Alianzas Estratégicas

- Diferentes vendors compartiendo IOCs

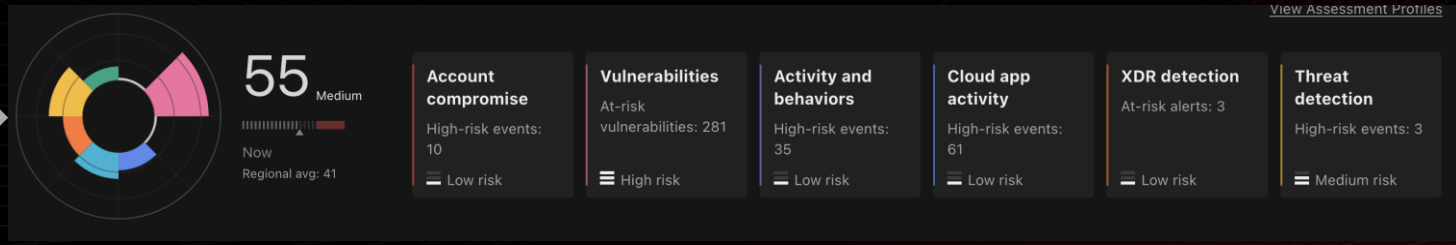
XDR nativo



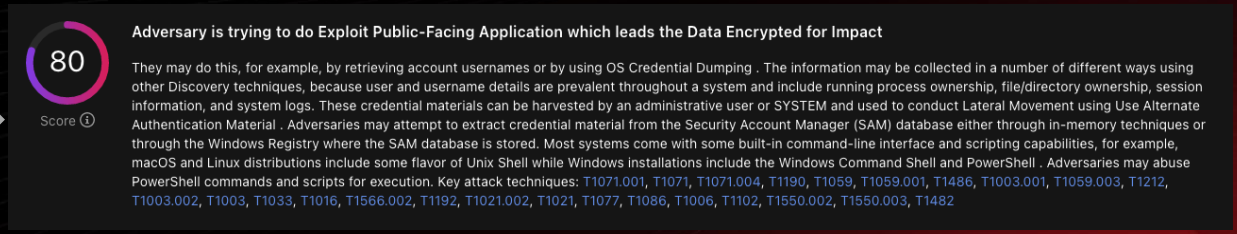
Arquitectura especialmente diseñada

- Correlación de telemetría y detecciones multivector con tecnología nativa.

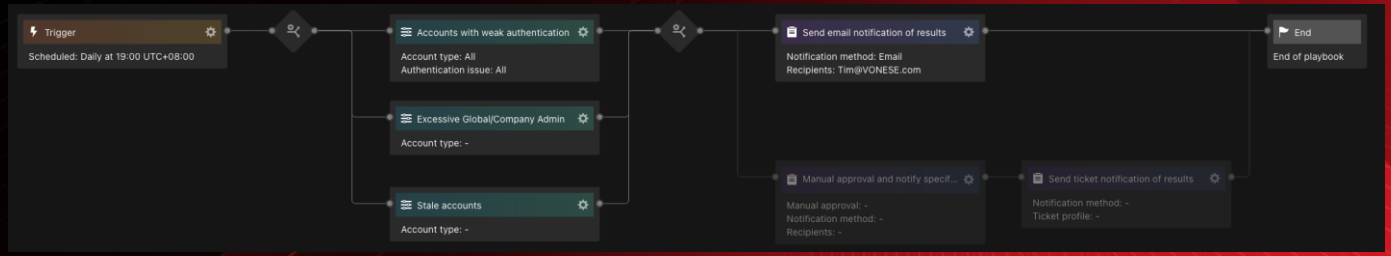
X→A→



D→B→



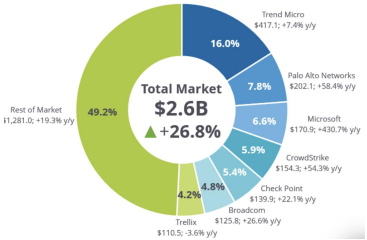
R→C→



Líderes en ciberseguridad

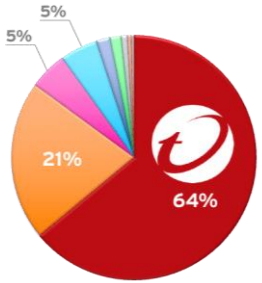
IDC Worldwide Cloud Workload Security Market Shares

May 2023



Omdia Global Vulnerability Research and Discovery

2022 Edition



Forrester Wave™: Endpoint Detection and Response

Q2, 2022

Forrester New Wave™: Extended Detection and Response (XDR)

Q4, 2021

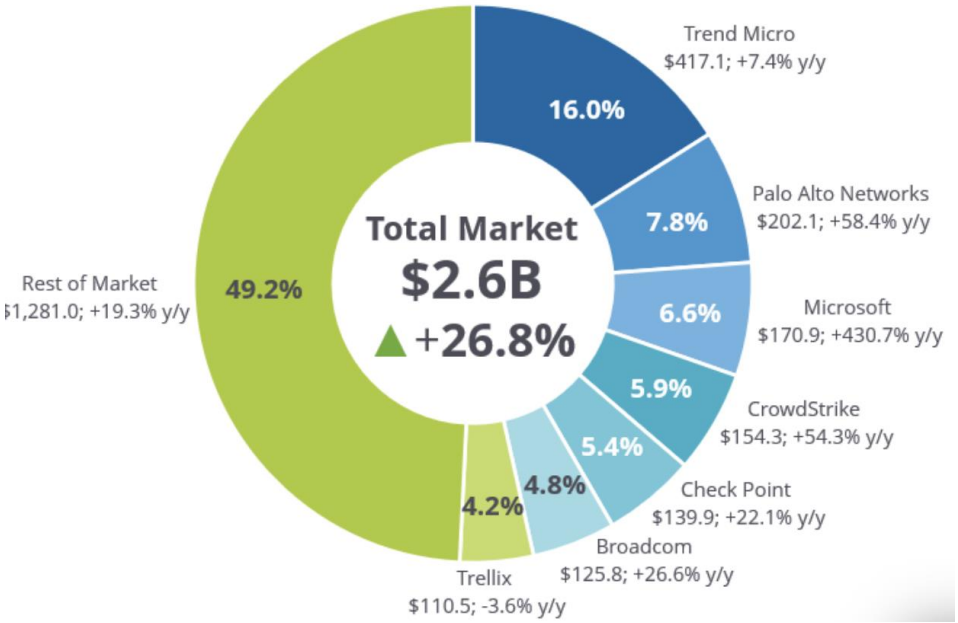
Forrester Wave™: Network Analysis and Visibility

Q2, 2023

Líderes en ciberseguridad

IDC Worldwide Cloud Workload Security Market Shares

May 2023



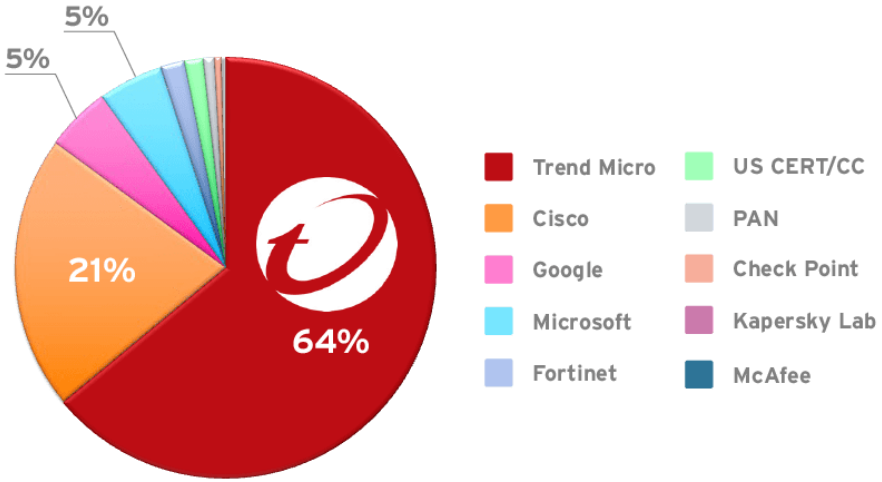
Omdia

Líderes en ciberseguridad

Quantifying the Public Vulnerability Market

2022 Edition

Omdia Research: Quantifying the Public Vulnerability Market: 2022 Edition



Challeng

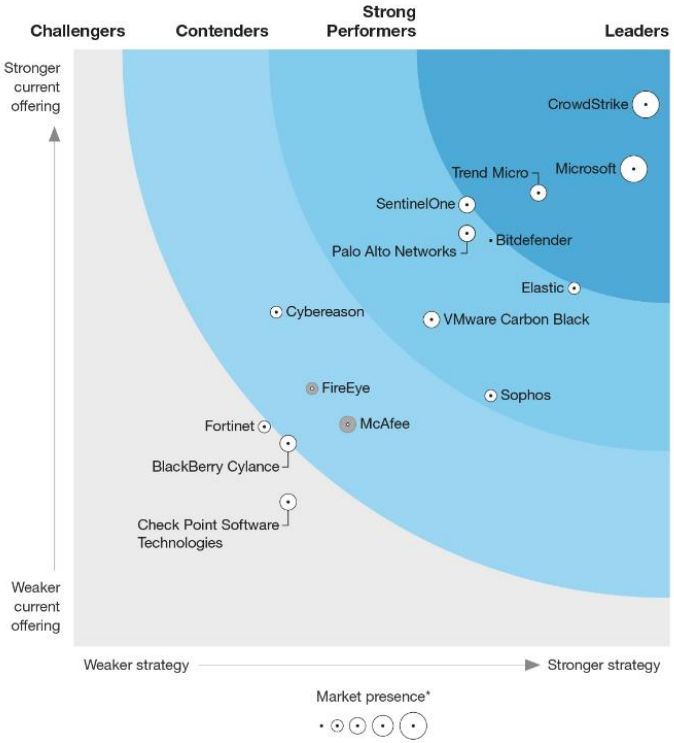
Stronger current offering

Weaker current offering

Líderes en ciberseguridad

Forrester Wave™: Endpoint Detection and Response

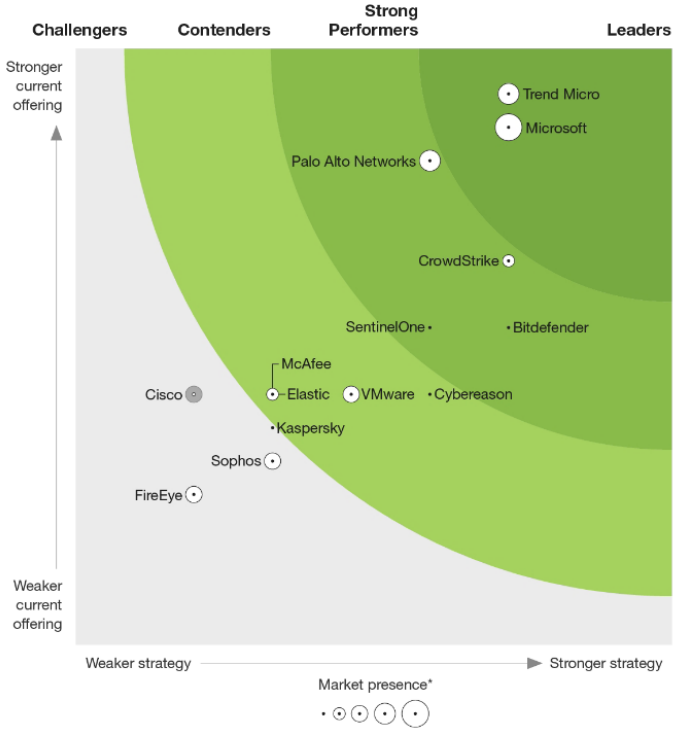
Q2, 2022

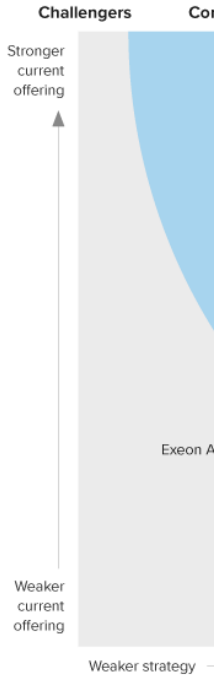


Líderes en ciberseguridad

Forrester New Wave™: Extended Detection and Response (XDR)

Q4, 2021





Líderes en ciberseguridad

Forrester Wave™: Network Analysis and Visibility

Q2, 2023

Alineados con el CCN

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11.0
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
Descripción	

Deep Discovery Inspector	
Versión	6.5.1129
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	N/A
Revisión de Validez	16/05/2026

TippingPoint Threat Protection System	
Versión	5.5.5
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Certificado:

- Endpoint/Servidores.
- NDR.
- IPS.

En Curso:

- IPS OT.
- Correo.

¡GRACIAS!