



El ABC de la Cyberseguridad



Jesús Gayoso Cuesta
Sales Engineer.

Delivery



Attacker



Callback phishing

Installation



Remote desktop
malware



Qakbot



Adfind



RDPEnable



Cobalt Strike



RClone



NetScan



PC Hunter



Process Hacker



GMER



Power Tool

Payload



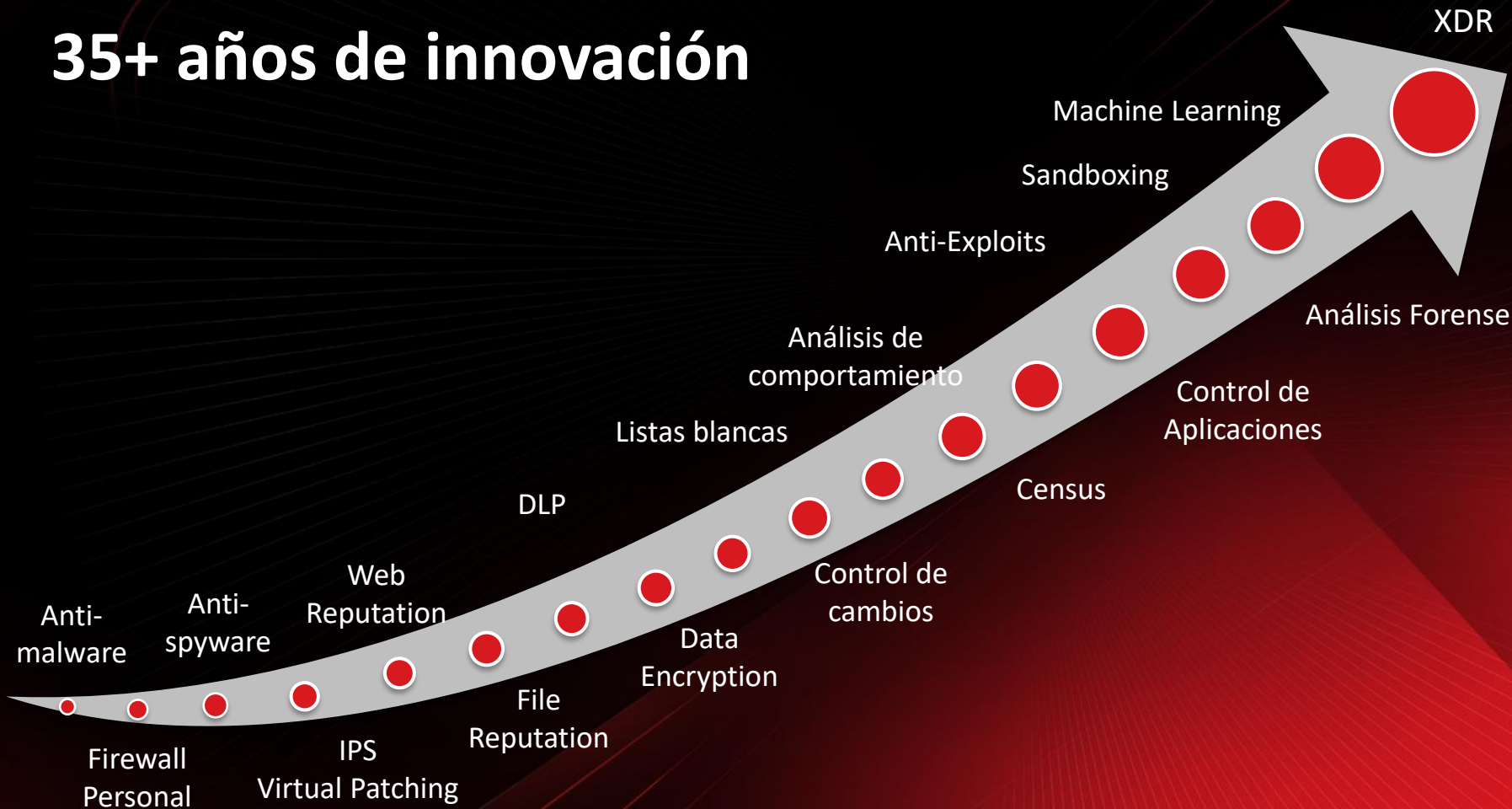
Psexec



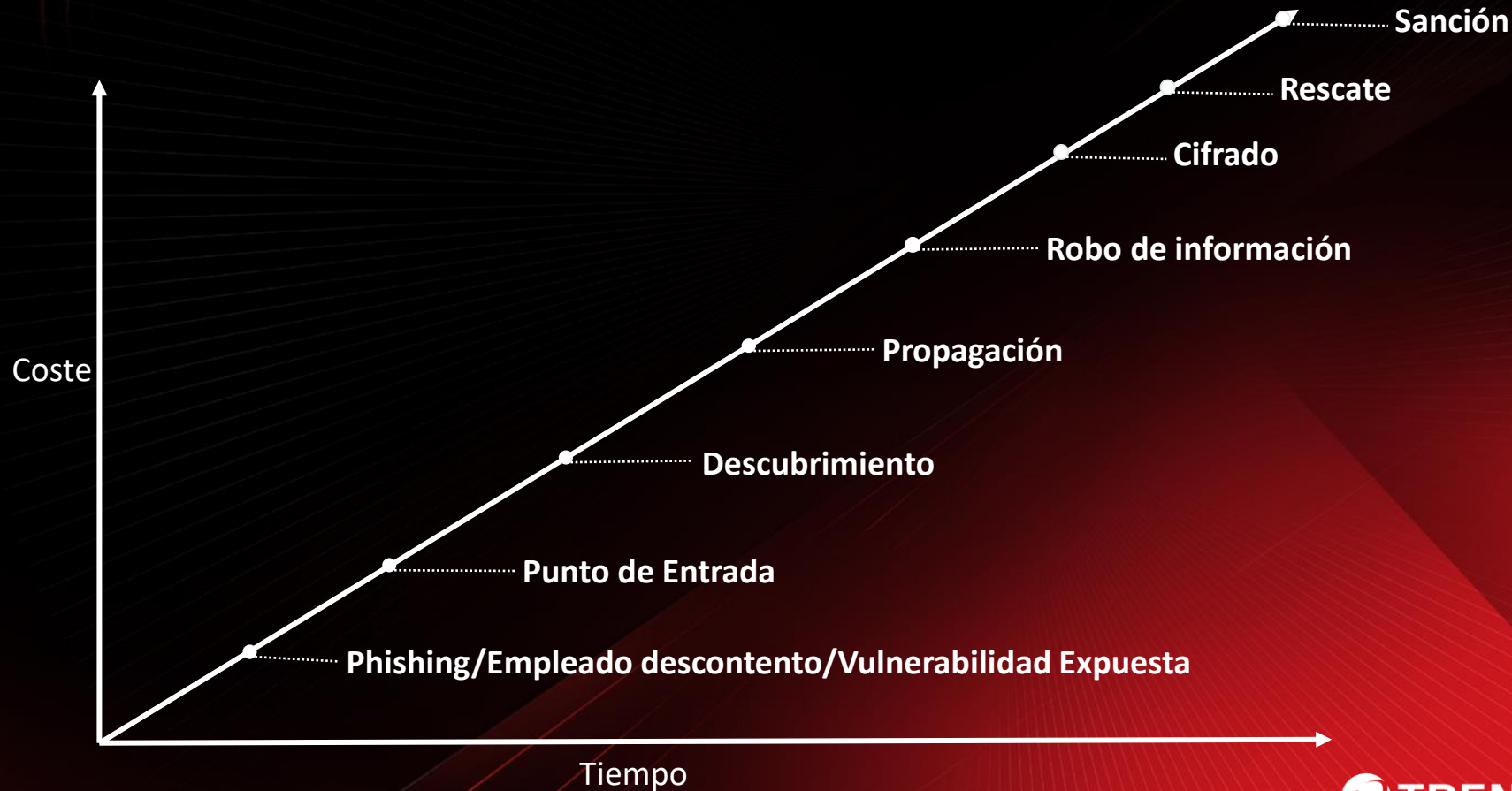
Royal Ransomware

©2023 TREND MICRO

35+ años de innovación



Coste = Cómo x Cuándo



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Analisis de la postura de seguridad.

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

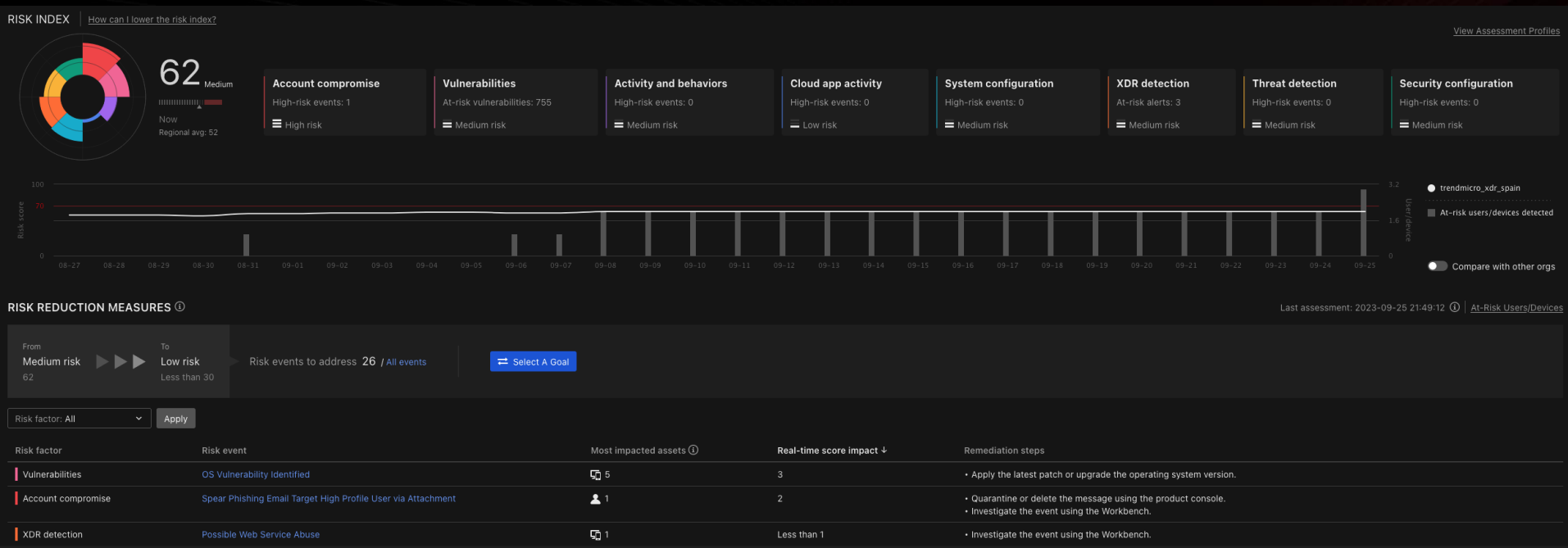
AI Native Foundation

Generative AI • Custom LLM • Machine Learning

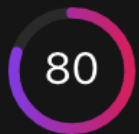
Managed Services

Ecosystem Integration

Análisis de la postura de Seguridad.



Bloqueo y detección del incidente.



Score ⓘ

Adversary is trying to do Exploit Public-Facing Application which leads the Data Encrypted for Impact

They may do this, for example, by retrieving account usernames or by using OS Credential Dumping . The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material . Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell . Adversaries may abuse PowerShell commands and scripts for execution. Key attack techniques: [T1071.001](#), [T1071](#), [T1071.004](#), [T1190](#), [T1059](#), [T1059.001](#), [T1486](#), [T1003.001](#), [T1059.003](#), [T1212](#), [T1003.002](#), [T1003](#), [T1033](#), [T1016](#), [T1566.002](#), [T1192](#), [T1021.002](#), [T1021](#), [T1077](#), [T1086](#), [T1006](#), [T1102](#), [T1550.002](#), [T1550.003](#), [T1482](#)

Status: All	Created: All	Model: All	Workbench ID, Endpoint, User, Email	Apply	
<input type="checkbox"/>	Score ↓ ⓘ	Workbench ID	Model	Model severity	Rela
<input type="checkbox"/>	66	WB-10253-20220325-00019	Targeted Attack Detection: Cobalt Strike - C&C Callback Traffic (Domain)	High	Simi
<input type="checkbox"/>	64	WB-10253-20220324-00034	Credential Dumping via Mimikatz	High	Simi
<input type="checkbox"/>	47	WB-10253-20220324-00038	Potential Information Gathering	Medium	Coll
<input type="checkbox"/>	47	WB-10253-20220323-00013	Suspicious Web Access After Suspicious Email	Medium	End

Bloqueo y detección del incidente.

Summary

Early Indicator of Conti Ransomware Attack

Multiple endpoint detections were found which is a potential indicator of being used by Conti ransomware as delivery.

Score: 71

Impact scope: 8 1

Created: 2021-12-10 22:38:36

Highlights

Possible Cobalt Strike Connection

Technique: T1071.001 - Application Layer Protocol, Web Protocols

T1071.004 - Application Layer Protocol, DNS

T1071 - Application Layer Protocol

Malware name: EICAR COBALTSTRIKE - HTTP (Response)

🕒 2021-12-10 22:35:08 | [View event](#)

🌐 (interestedIp) 10.50.1.133

💻 (src) 23.82.128.116

📄 (deviceDirection) inbound

📄 (clientFlag) dst

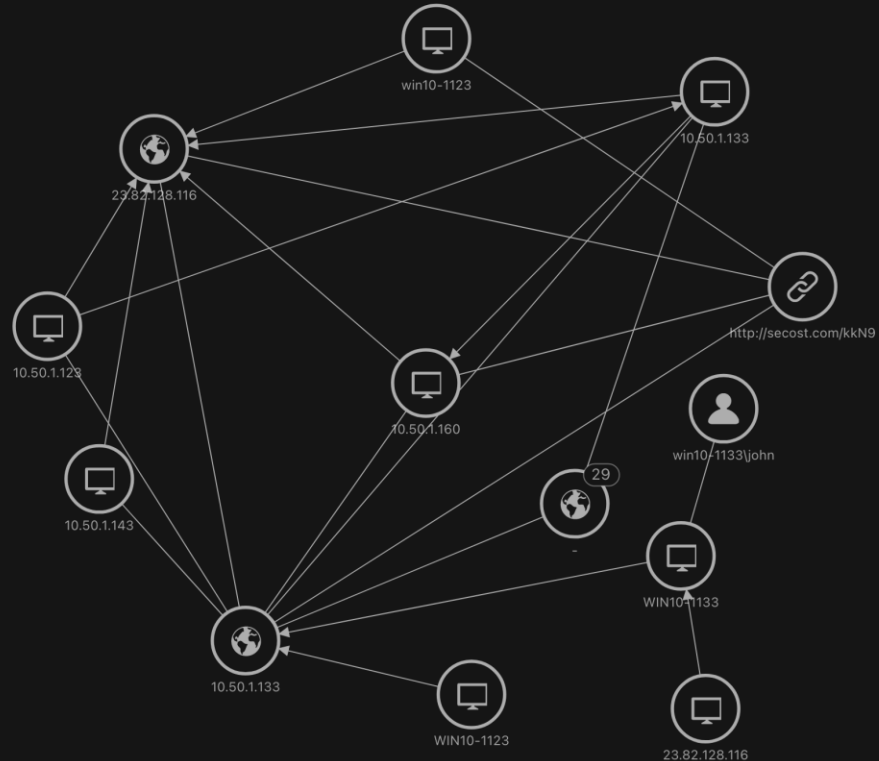
📄 (pAttackPhase) Command and Control Co...

📄 (ruleId) 4155

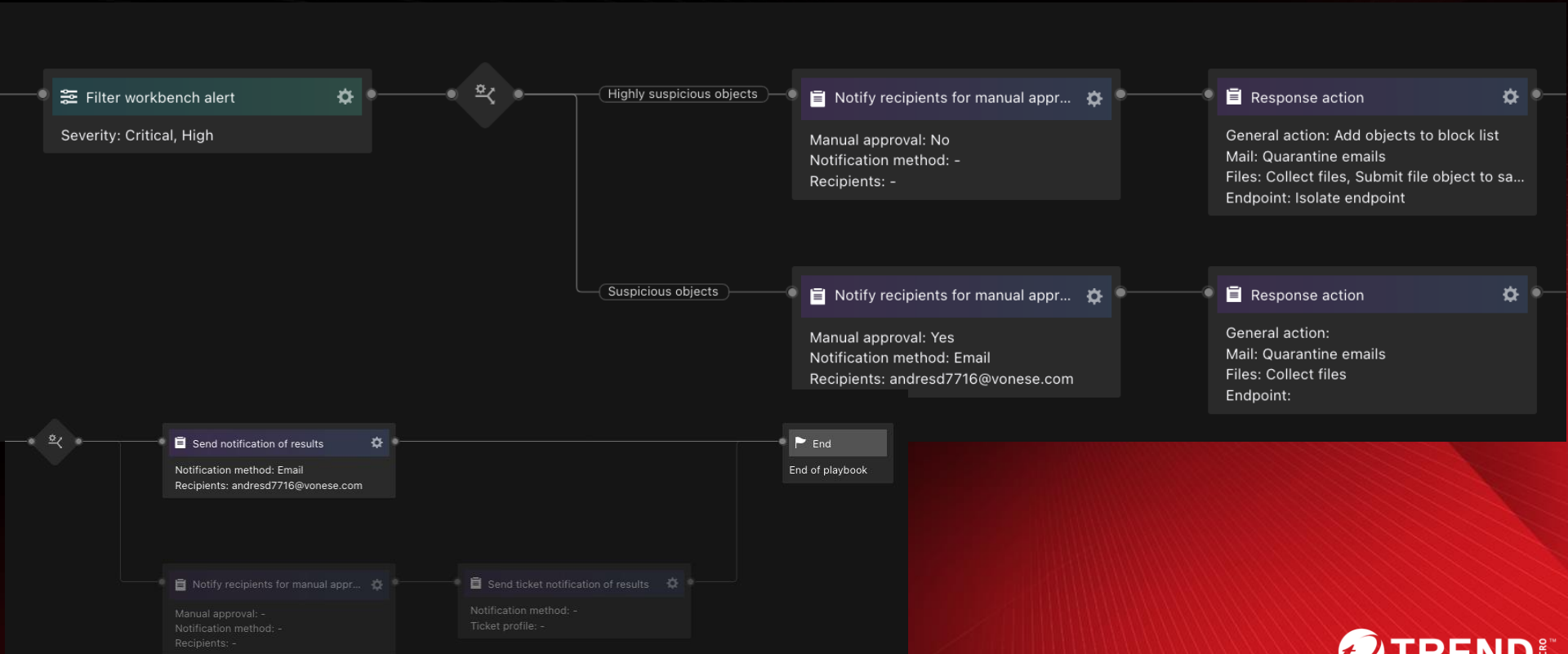
📄 (app) HTTP

💻 (peerHost) 23.82.128.116

🌐 (peerIp) 23.82.128.116



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

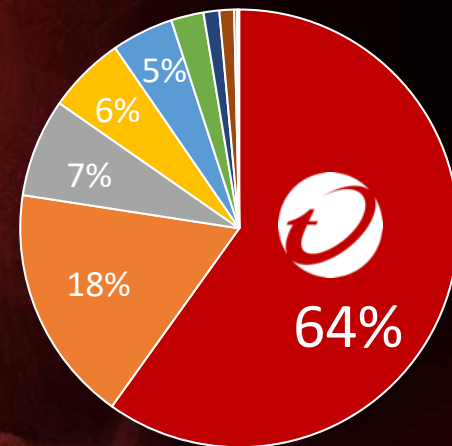
Aplicaciones de escritorio

Clientes de correo

Navegadores Web

Antivirus

Etc...



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

A Platform Approach to Layered Security

LEGEND



Known Good Data



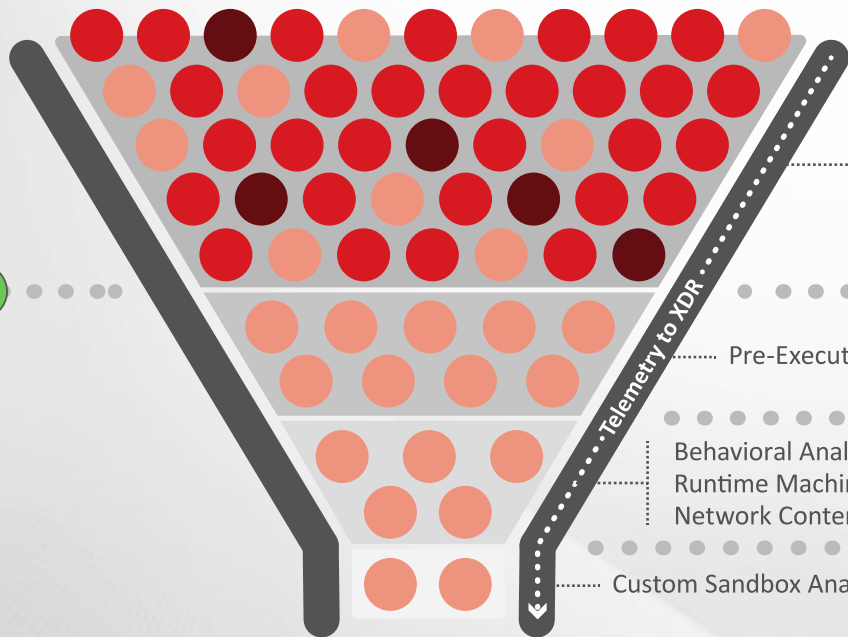
Known Bad Data



Unknown Data



Noise Cancellation



Intrusion Prevention (IPS) & Firewall
Early Zero-Day Protection
Exploit Prevention & File/Web Reputation
Variant Protection
Application Control
Integrity Monitoring

Pre-Execution Machine Learning

Behavioral Analysis
Runtime Machine Learning
Network Content Correlation

Custom Sandbox Analysis

Investigation & Response



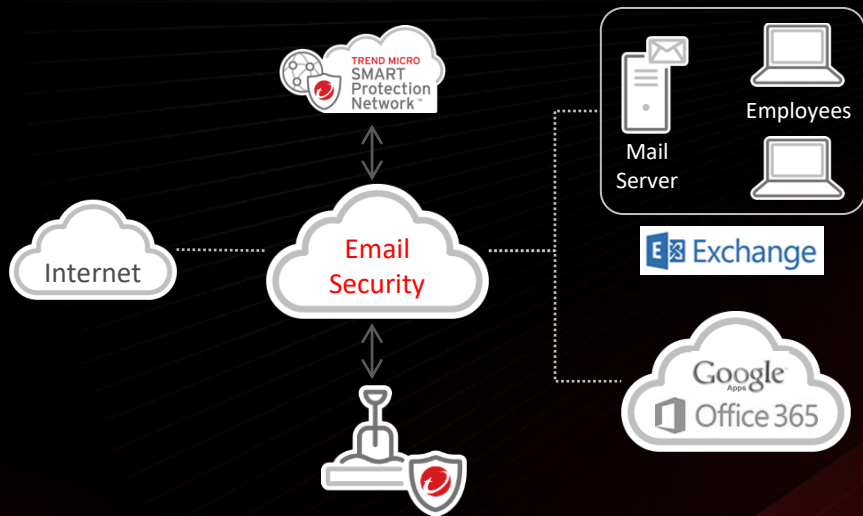
Safe files & actions allowed



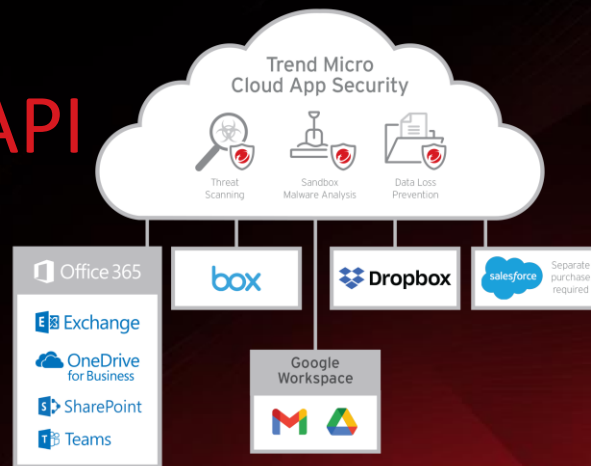
Malicious files & actions blocked

Protección de correo y telemetría

MTA



API



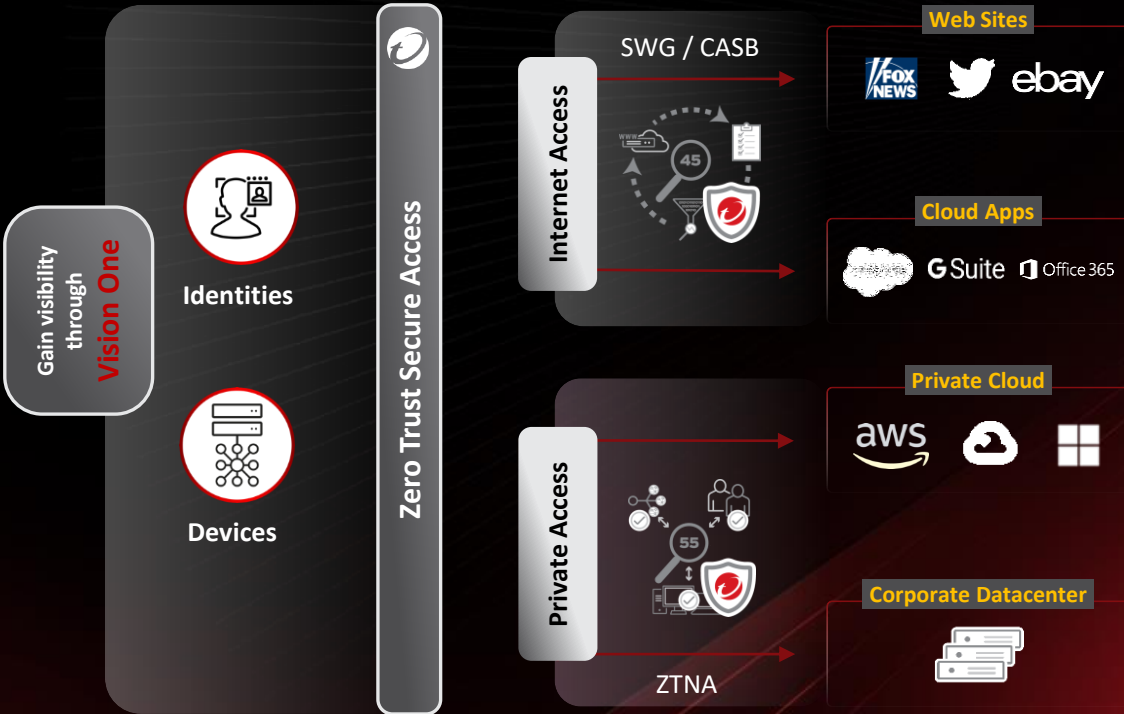
Email Sensor

The screenshot shows the "Email Sensor" configuration interface. The main heading is "Enable XDR messaging capability on Gmail". Below this, there is a step-by-step guide:

- 1. **Install the Trend Micro Cloud App Security app.** (Click here)
- 2. **Grant Cloud App Security permission on the APIs requested to access your Gmail related service data.** (Click here)

Additional text includes: "Experience X power", "Get the power of XDR for Gmail accounts. Gain a more complete view of attacks by leveraging email activity data for correlated detection and investigation.", and "Share this with your email administrator". A "Set up for Microsoft 365" button is visible at the bottom.

Zero Trust Secure Access - **Secure Service Edge**



Evolución del proxy.
Gestión de riesgos y aplicación de políticas dinámicas 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

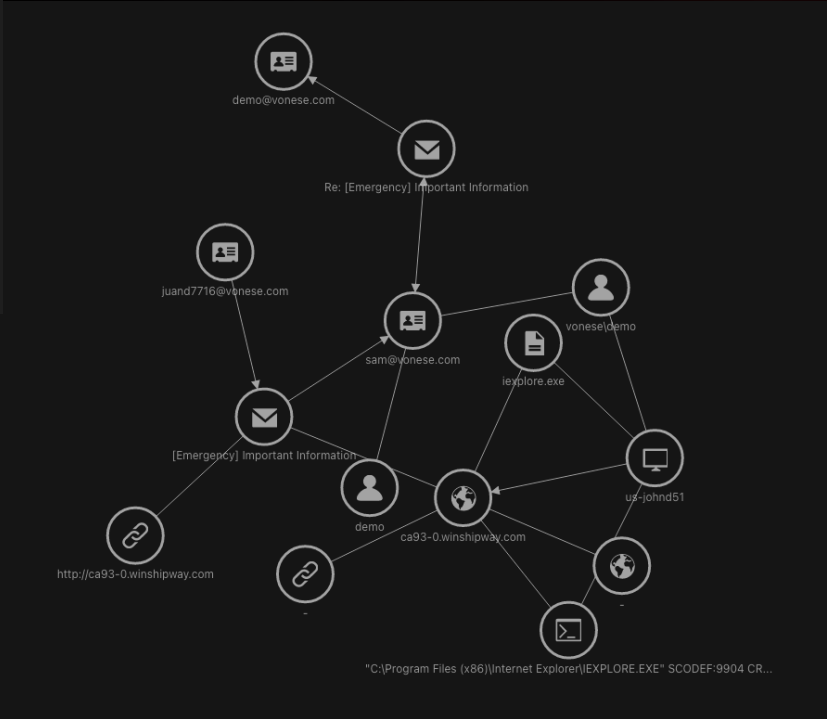
Summary  

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/pe erIp	* 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

Trend Micro Vision One™ | Response Management

Task List Custom Scripts

Collect File ▾ Task status: Successful ▾ Action: All ▾ Target type: Network ▾ Created by: All ▾

Task ID ⓘ	Action	Target
▶ 3 ✔ 00134542	Collect Network Analysis Package	🌟 File - 0FCB5B69B61A340B9EC4D7489A21DDC0...
▶ 3 ✔ 00134538	Collect Network Analysis Package	🌟 File - 26DA7547C4ACB41FD18DE1DD11FC24B1...
▶ 1 ✔ 00134537	Collect Network Analysis Package	🌟 PCAP file - d70467c3-b0cc-4c91-8871-3409e56...
▶ 1 ✔ 00134513	Collect Investigation Package	🌟 Investigation package - 34F917AABA5684FBE5...
▶ 1 ✔ 00134489	Submit for Sandbox Analysis	🌟 File - D922168ECBED07452453568F61B68CF52...
▶ 1 ✔ 00134461	Collect Network Analysis Package	🌟 PCAP file - f1060aa6-e2cd-4b3f-9e71-68018fa3...
▶ 2 ✔ 00134460	Collect Network Analysis Package	🌟 File - 0FCB5B69B61A340B9EC4D7489A21DDC0...

Vision One™ search

View History

etections ▾ productCodepdi

SEARCH RESULTS OBTAINED 83.04% DATA (959 EVENTS) Query More

logged	681943
fileType	APC
fileSize	Yes
hostName	172.22.9.150
hostSeverity	1
interestedGroup	Default
interestedHost	172.22.9.150
interestedIp	172.22.9.150
isHidden	Yes
logId	C15E8687D06F-4EEA998-3016-3608-58E3-DD1-3-0-W-ISOV1-en_219241
malware	MALWARE
malware	Malware
malwareMapping	11510 (1A0000)
malwareVersion	v9
overSsl	Not over SSL/TLS
pAttackPhase	Lateral Movement
pComp	CM
peerSID	87205780-653e-4d6b-a869-317f...
peerGroup	Default
peerHost	10.1.119.93
peerId	10.1.119.93

GENERAL

Copy to Clipboard

SEARCH

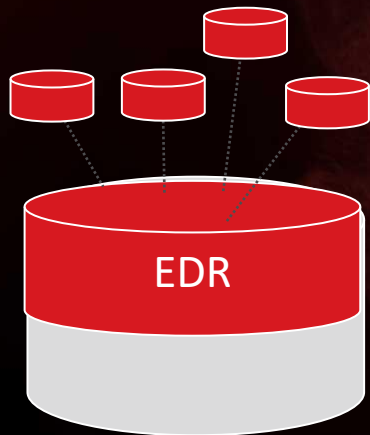
Google

RESPONSE

Collect PCAP File

Diferentes enfoques de XDR en el Mercado

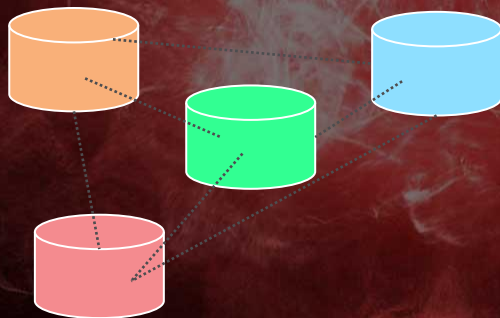
Extended EDR



Foco en el Endpoint

- Telemetría y detecciones recogidas del endpoint.

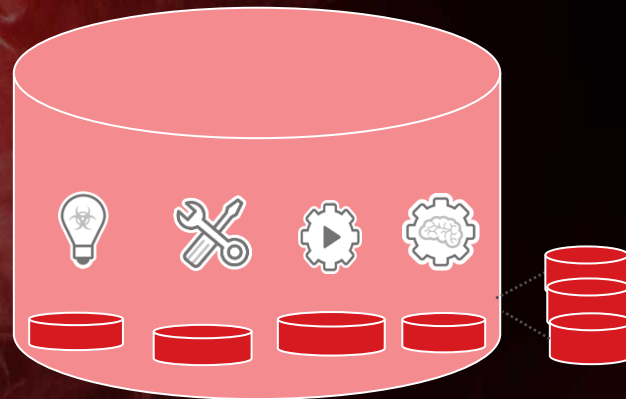
XDR Con Alianzas



Alianzas Estratégicas

- Diferentes vendedores compartiendo IOCs

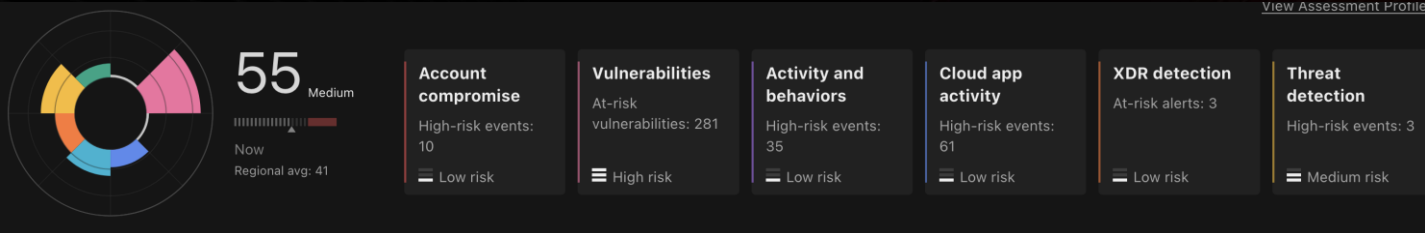
XDR nativo



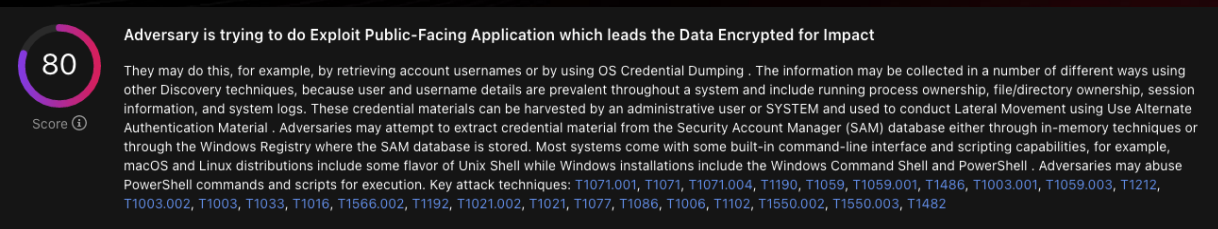
Arquitectura especialmente diseñada

- Correlación de telemetría y detecciones multivector con tecnología nativa.

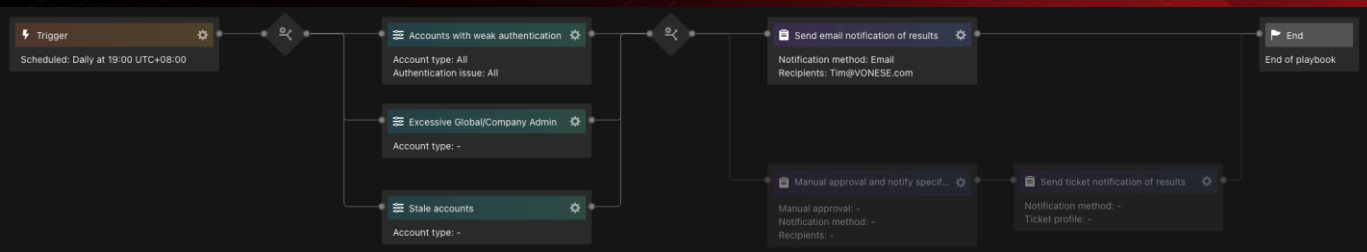
X → A



D → B



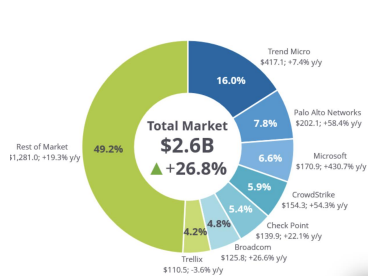
R → C



Líderes en ciberseguridad

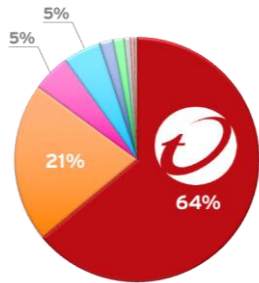
IDC Worldwide Cloud Workload Security Market Shares

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

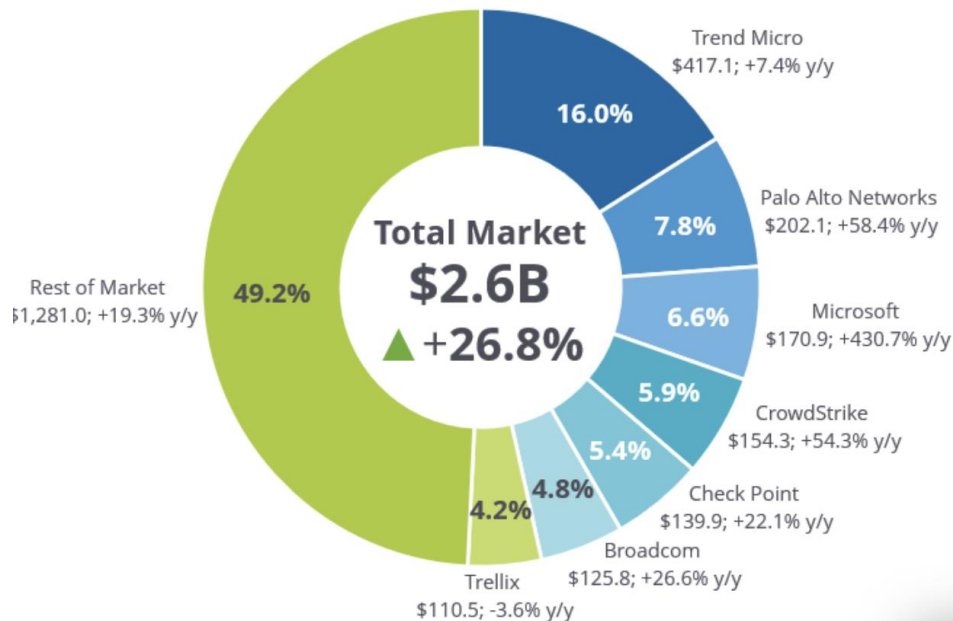


The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Líderes en ciberseguridad

IDC Worldwide Cloud Workload Security Market Shares

May 2023



Omdia

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

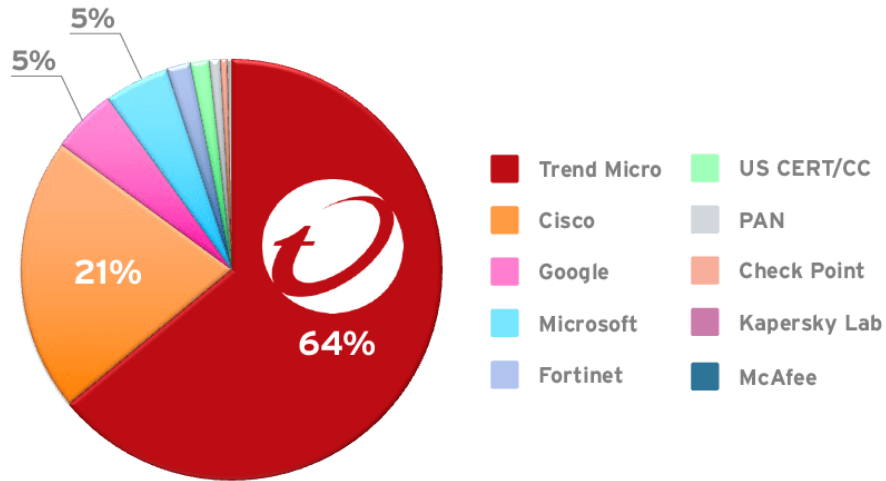


Líderes en ciberseguridad

Quantifying the Public Vulnerability Market

2022 Edition

Omdia Research: Quantifying the Public Vulnerability Market: 2022 Edition



Challenging

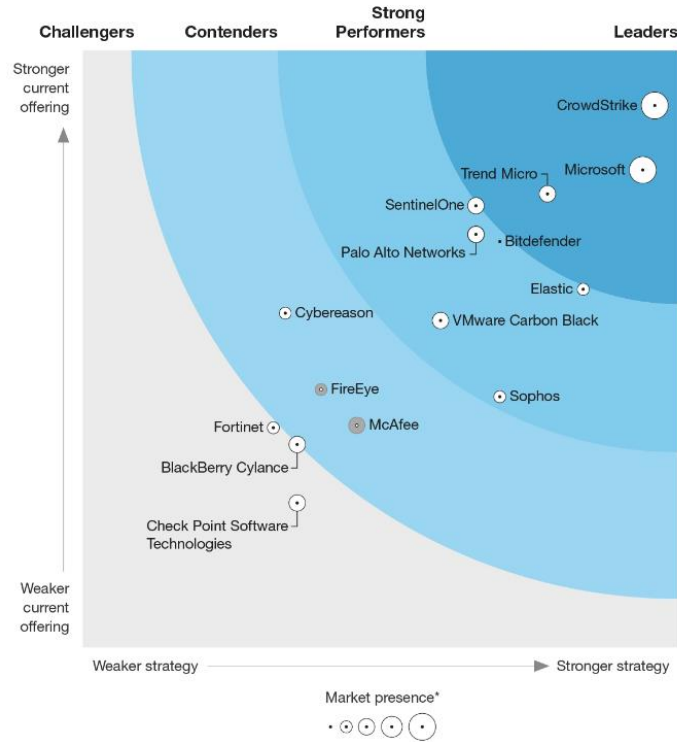
Stronger current offering

Weaker current offering

Líderes en ciberseguridad

Forrester Wave™: Endpoint Detection and Response

Q2, 2022

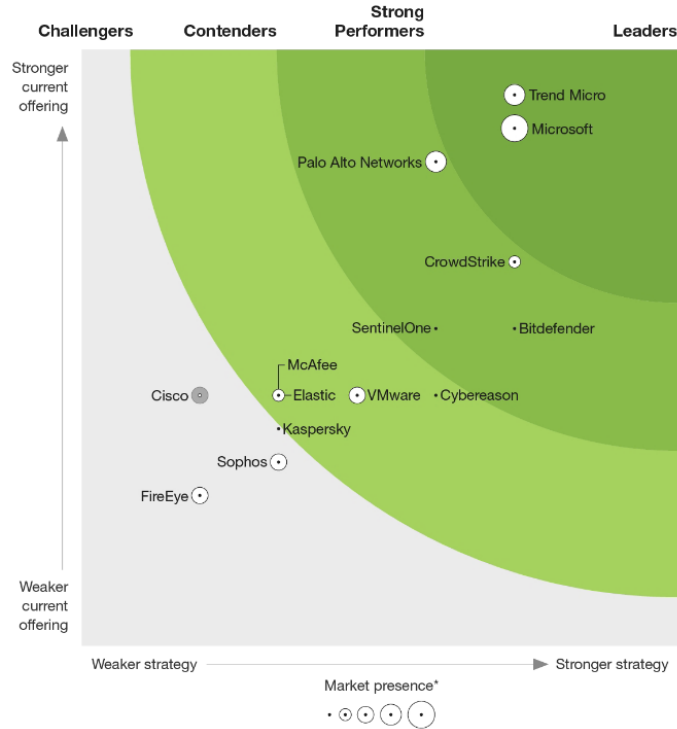


The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Líderes en ciberseguridad

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

Q4, 2021



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Líderes en ciberseguridad

Forrester Wave™: Network Analysis and Visibility

Q2, 2023



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

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!