



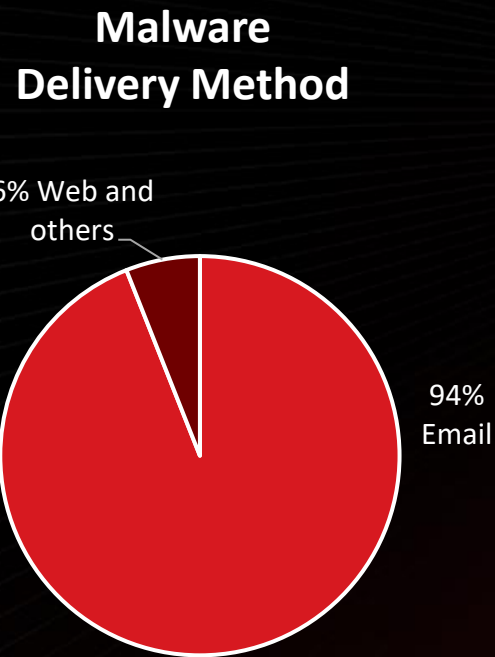
Email solutions
Trend Micro



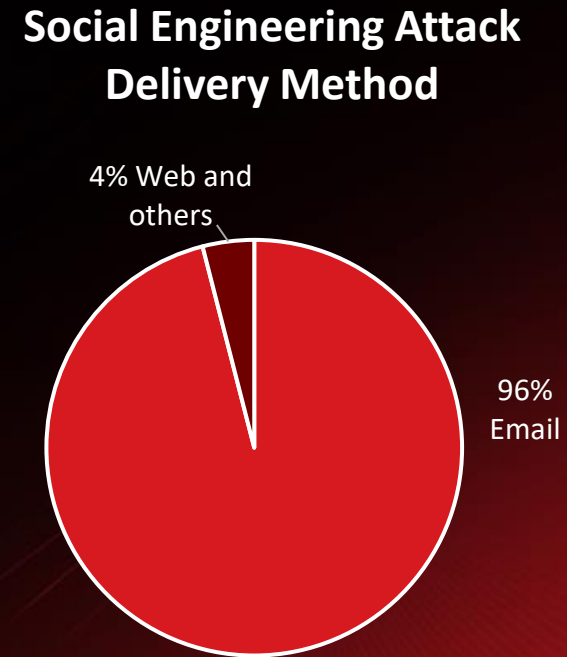
Objetivos del Curso

- Definir las Problemáticas que aplican a la Infraestructura de Correo comunes a cualquier organización.
- **Features de Detección en Tecnologías TrendMicro**
- Administración e Interacción con Herramientas de Correo.
- Monitoreo & Administración de las cuarentenas, incluyendo **End-User Quarantine**.
- Generación de **Reportes** y **Logs** de eventos desde la consola.

La mayoría de los ciberataques provienen del correo electrónico



Source: Verizon DBIR 2019



Source: Verizon DBIR 2020

Business Email Compromise (BEC) Attacks



El impostor envía un correo electrónico a "Max" haciéndose pasar por "Eva"

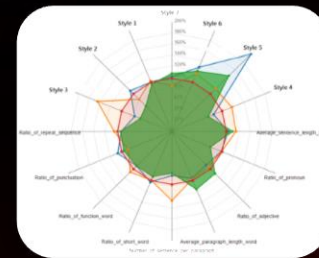
Max,

¿Cómo estás? Hay algo en lo que necesito tu ayuda, avísame si estás menos ocupado para darte los detalles

Saludos,
Eva

Office 365

Exchange



El nombre del remitente del correo electrónico entrante coincide con el ejecutivo pero no con el estilo de escritura



Usuario suplantado, "Eva"



Confirmación (opcional)



Advertencia



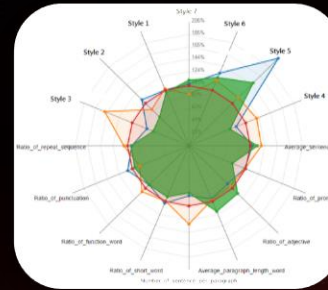
Destinatario "Max"

AI based BEC Detection

Behavior + Intention analysis

Behavior	Routing behavior
	Cousin domain
	High-profile user similarity
	...
Intention	Financial impact
	Urgency
	...

Mimics the decision making of a security expert



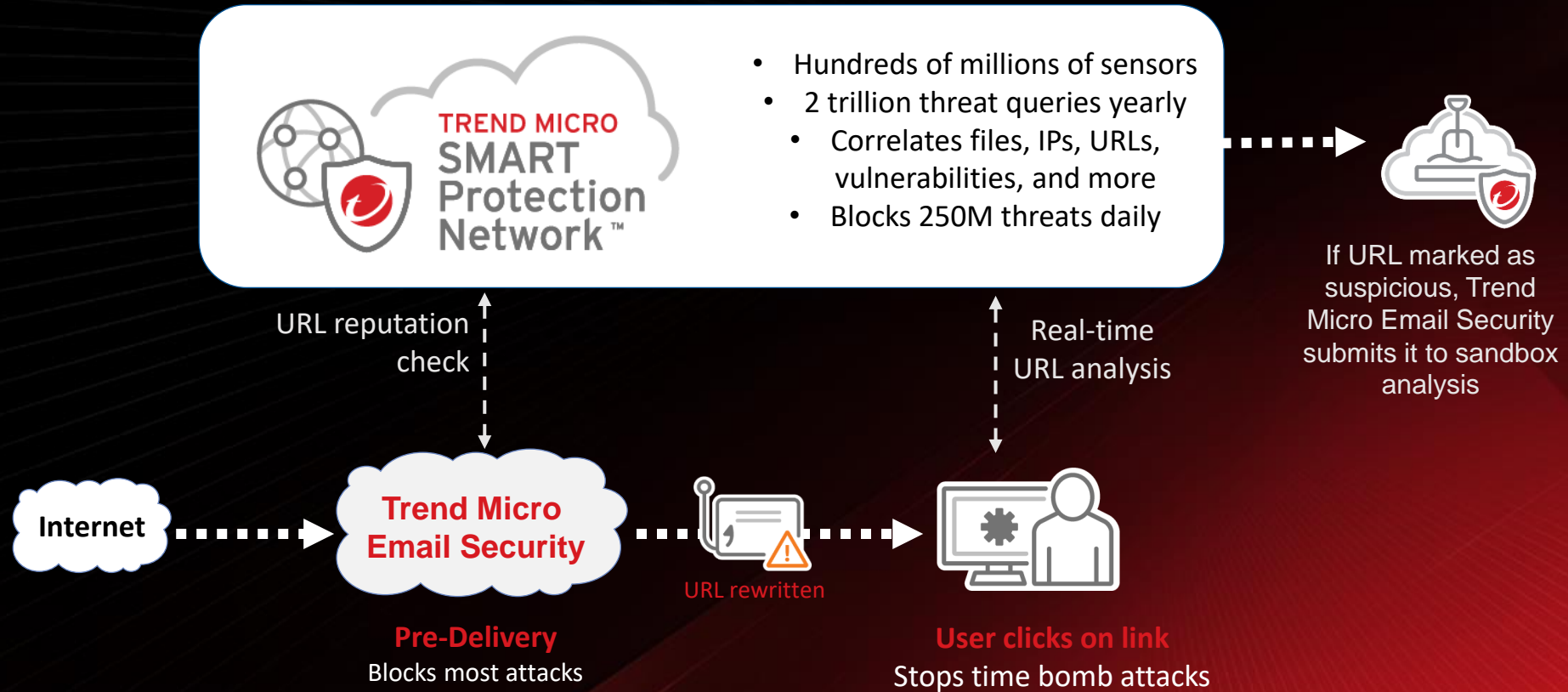
Authorship analysis

Compares a suspected impersonation to AI model of high-profile user's writing style

WRITING STYLE DNA

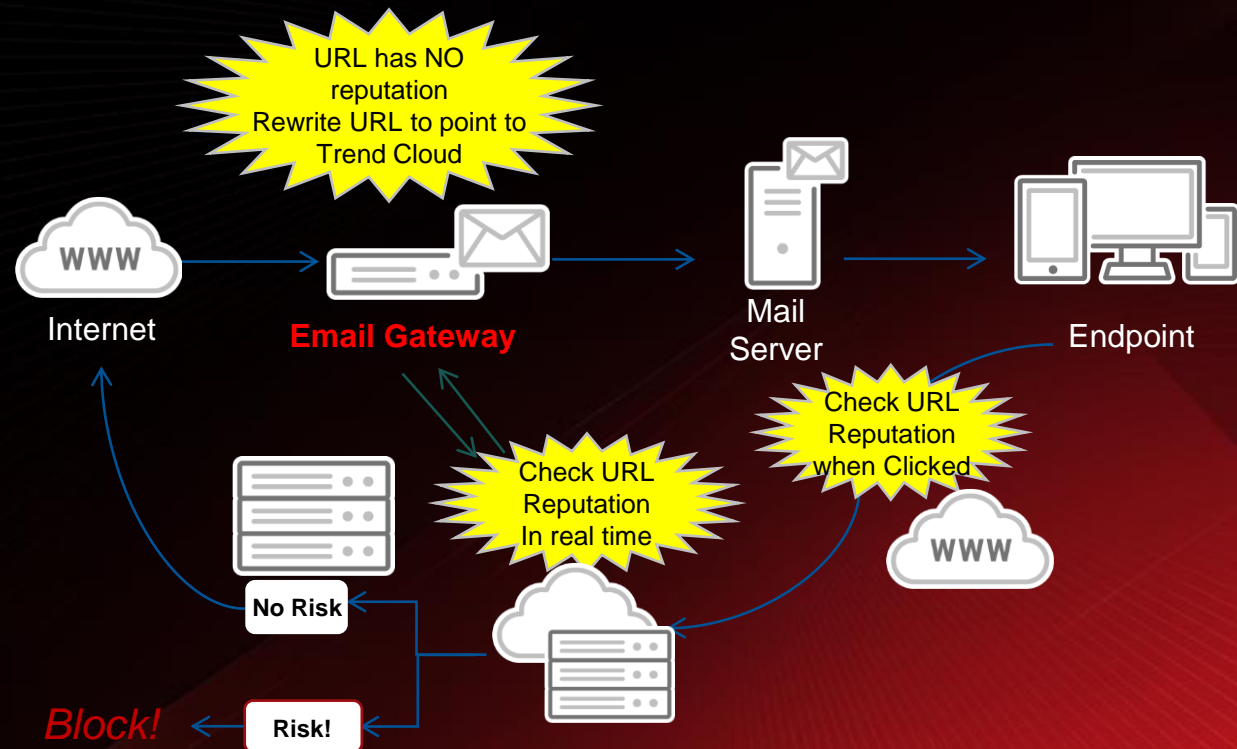


Malicious URL Protection



Threat detection – URL Time Of Click

Evalúa las URL no sólo cuando se reciben por primera vez sino también cuando se accede a ellas.





SMART: Unique Blend to Protect Email

LEGEND



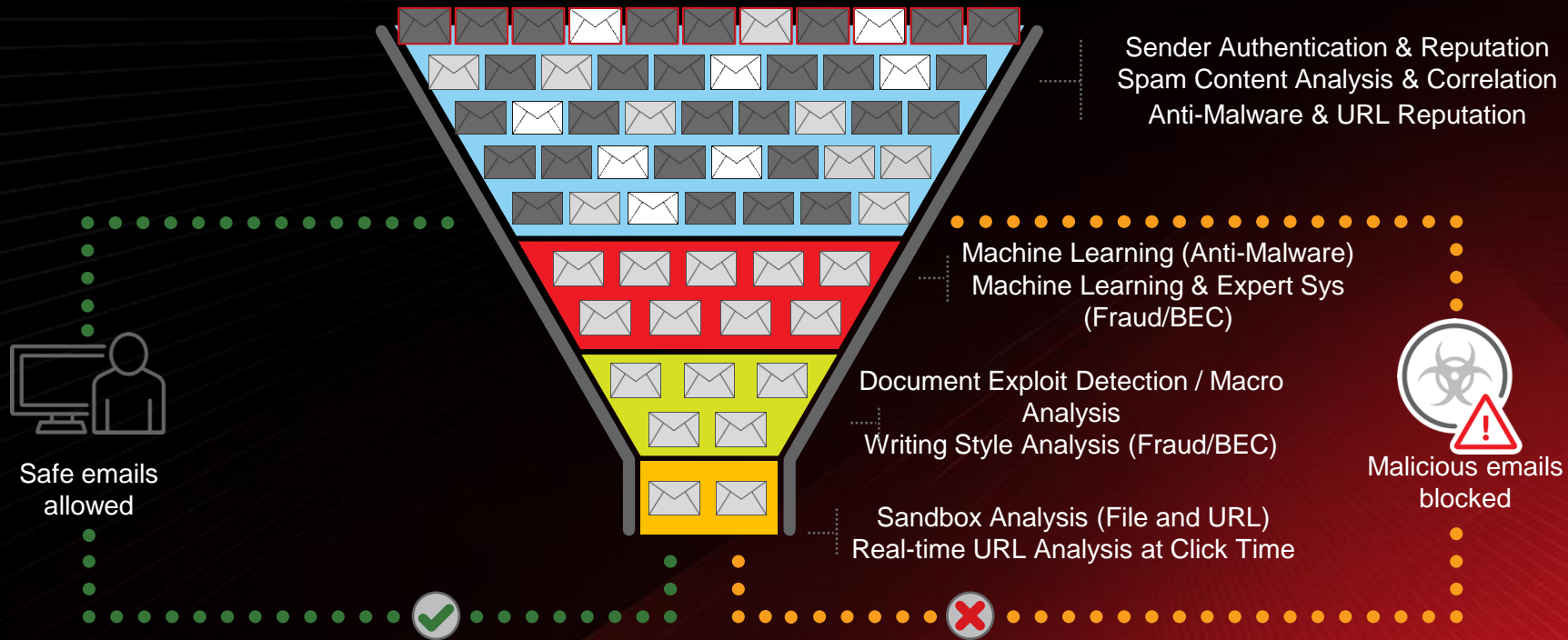
Known Good



Known Bad



Unknown



Trend Micro Email Security Portfolio



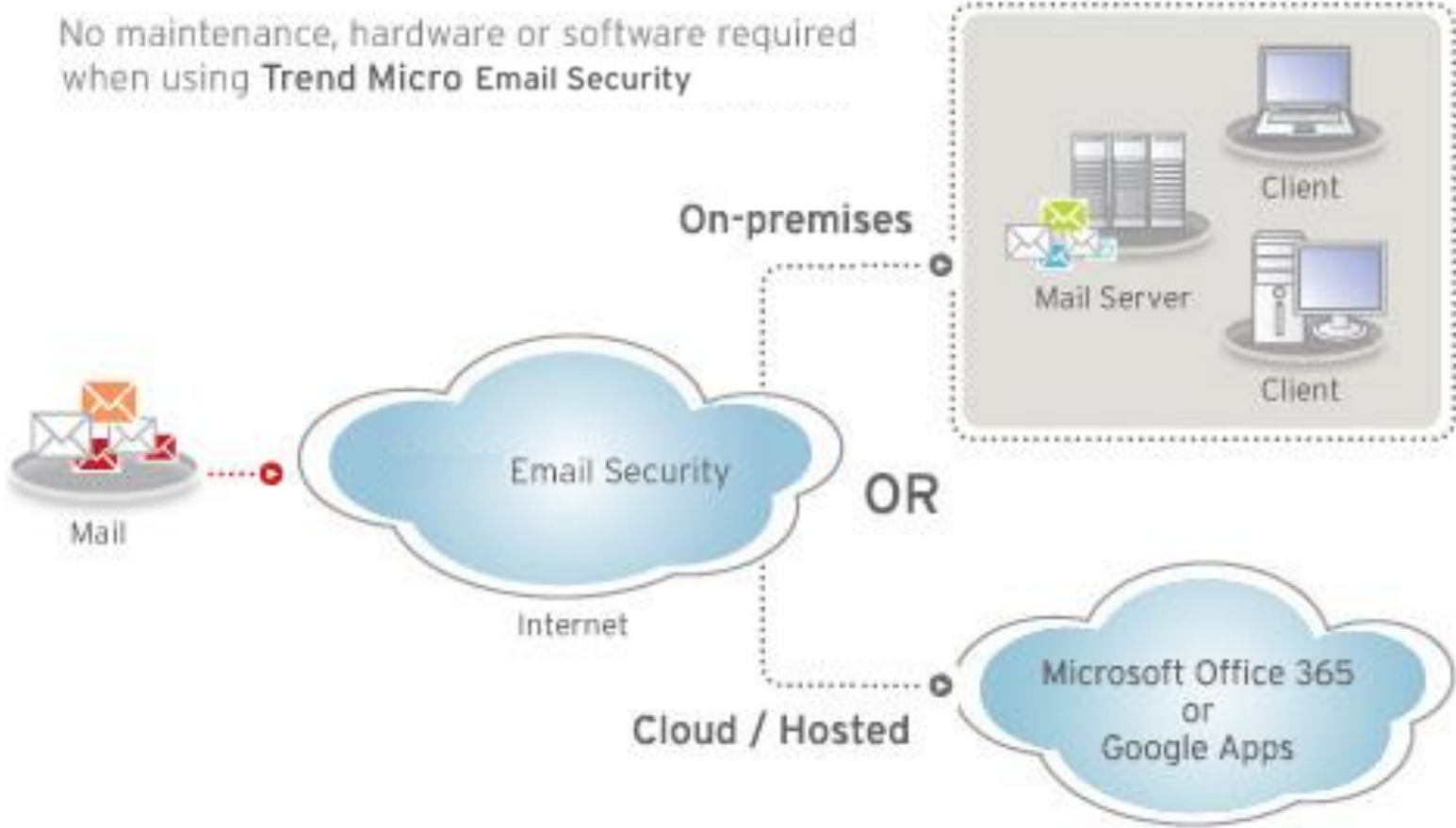
Trend Micro Email Solutions




Trend Micro Email Security (TMES)

Deploy TMES (SaaS)

No maintenance, hardware or software required when using Trend Micro Email Security




Deploy TMES (SaaS)

Inbound Servers 

* @demo.4ems.net in.tmes-anz.trendmicro.com 25 10 - +

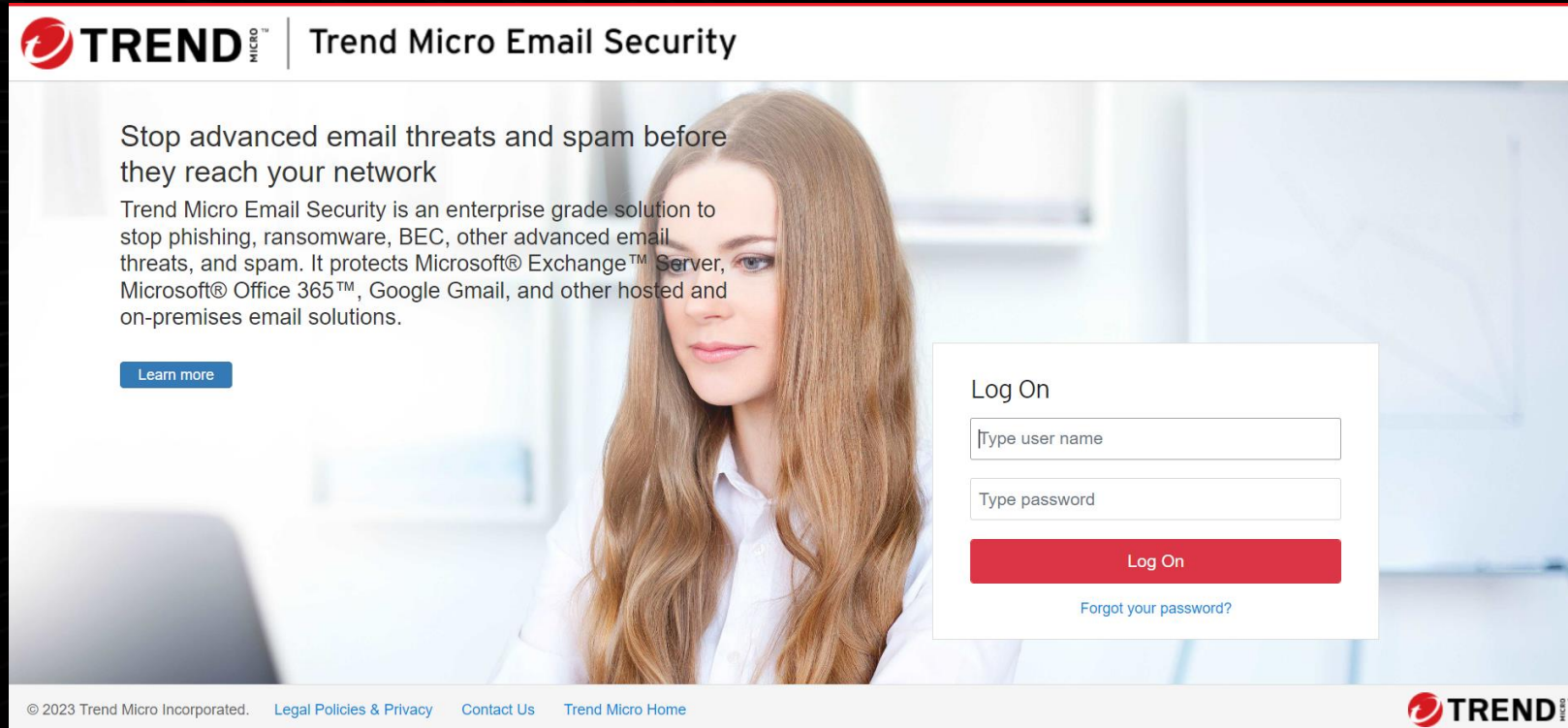
Inbound servers verified. Check the [detailed configurations](#).

- 1 Configure your firewall to accept email messages from the following Trend Micro Email Security servers:
 - 18.208.22.64/26
 - 18.208.22.128/25
 - 18.188.9.192/26
 - 18.188.239.128/26
- 2 Click **Test Connection**.
- 3 Point the MX records of your domain to the following Trend Micro Email Security server with the lowest preference value: 
tmemsdemo.in.tmes.trendmicro.com
- 4 Click **Verify**.

NOTE: It may take some time for DNS changes to take effect, and Trend Micro Email Security will periodically check the changes.

TMES

Consola Web de Administración



The screenshot shows the Trend Micro Email Security (TMES) web administration console. At the top left is the Trend Micro logo and the text "Trend Micro Email Security". The main content area features a woman with long brown hair looking at a laptop. To her left, there is a heading "Stop advanced email threats and spam before they reach your network" followed by a paragraph describing the product as an enterprise-grade solution for phishing, ransomware, and spam. Below this is a "Learn more" button. To the right of the woman is a "Log On" form with two input fields for "Type user name" and "Type password", a red "Log On" button, and a link for "Forgot your password?". The footer contains copyright information, legal policies, contact links, and the Trend Micro logo.

TREND MICRO | Trend Micro Email Security

Stop advanced email threats and spam before they reach your network

Trend Micro Email Security is an enterprise grade solution to stop phishing, ransomware, BEC, other advanced email threats, and spam. It protects Microsoft® Exchange™ Server, Microsoft® Office 365™, Google Gmail, and other hosted and on-premises email solutions.

[Learn more](#)

Log On

Type user name

Type password

Log On

[Forgot your password?](#)

© 2023 Trend Micro Incorporated. [Legal Policies & Privacy](#) [Contact Us](#) [Trend Micro Home](#) **TREND MICRO**

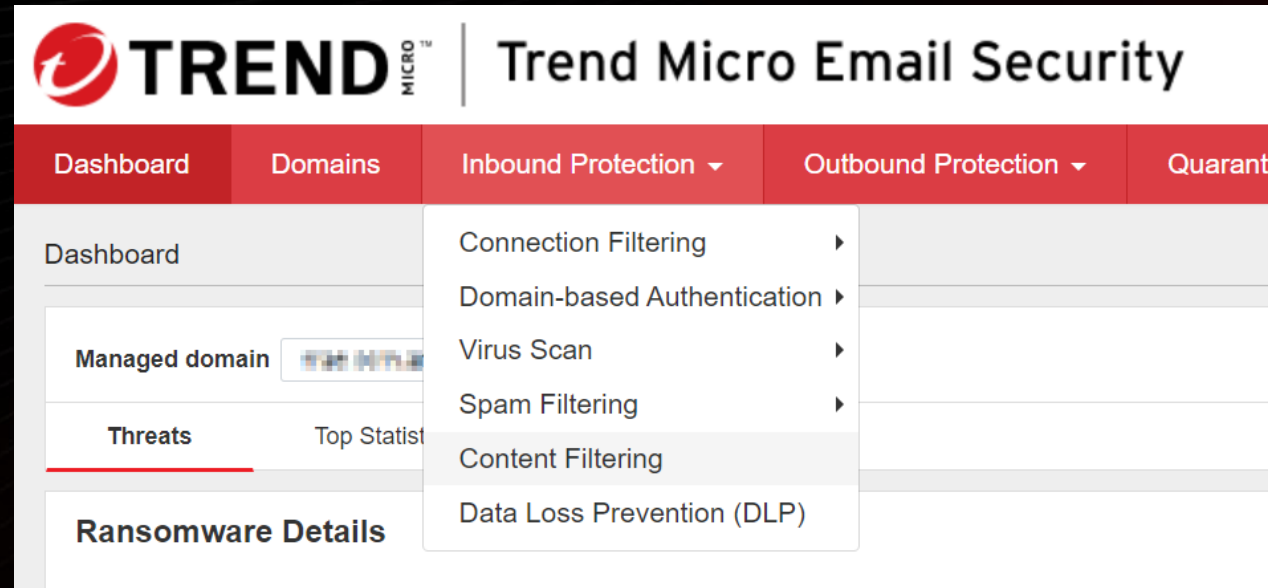
URL de Ingreso:

https://ui.tmes.trendmicro.com/en/index.html?_=1680706981104

TMES

Tipos de Políticas

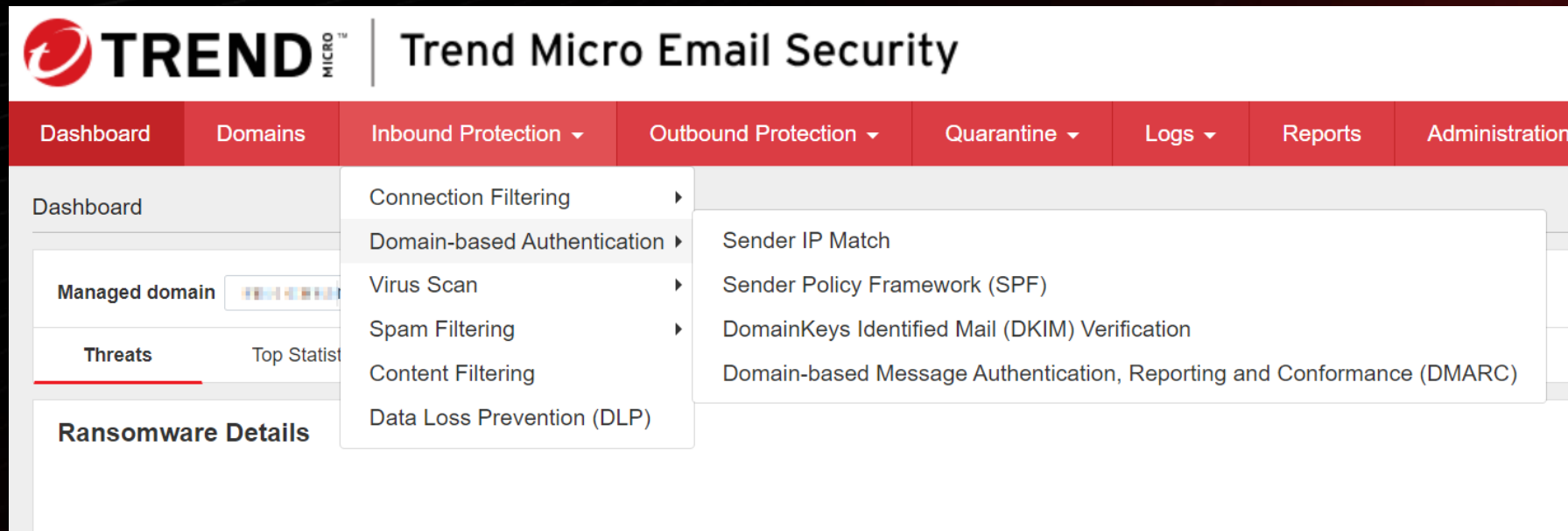
- Políticas divididas en “Protección Entrante o Protección Saliente” y subdivididas en distintas features de seguridad



Controles de Autenticación de dominios

Existen tres tipos de chequeos aplicables sobre ambas plataformas:

- **SPF**
- **DKIM**
- **DMARC**



The screenshot displays the Trend Micro Email Security dashboard. The top navigation bar includes 'Dashboard', 'Domains', 'Inbound Protection', 'Outbound Protection', 'Quarantine', 'Logs', 'Reports', and 'Administration'. The 'Domains' menu is open, showing a list of managed domains. The 'Domain-based Authentication' option is selected, revealing a sub-menu with the following items: 'Sender IP Match', 'Sender Policy Framework (SPF)', 'DomainKeys Identified Mail (DKIM) Verification', and 'Domain-based Message Authentication, Reporting and Conformance (DMARC)'. Other visible options in the 'Inbound Protection' menu include 'Connection Filtering', 'Virus Scan', 'Spam Filtering', 'Content Filtering', and 'Data Loss Prevention (DLP)'.

Email Reputation

- **Email Reputation** es una tecnología que valida las IP públicas contra una Base de Datos que contiene los senders de Spam “más conocidos” y se encuentra en la **SPN** (Smart Protection Network).

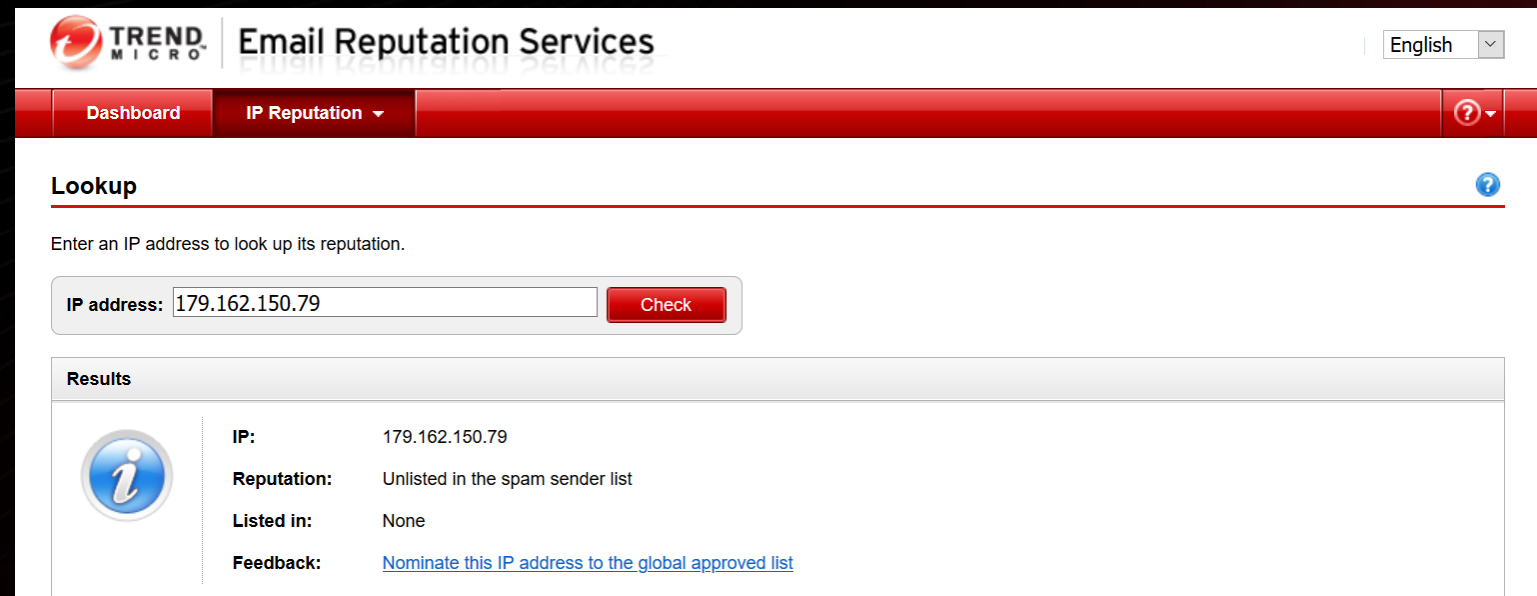
The screenshot shows the Trend Micro Email Reputation Service interface. At the top left is the Trend Micro logo and the text "Email Reputation Service". On the top right, there is a globe icon and a "Sign In" button. Below the header is a navigation bar with "Home", "IP Reputation ^", and "More Info v". The main content area features a search bar with a magnifying glass icon, the placeholder text "Ex. 127.0.0.1", and a red "Look Up" button. To the left of the search bar is a dropdown menu with three options: "Lookup", "Add to Global Approved List", and "Add to Global Blocked List". To the right of the search bar, the text reads "Worried about being spammed? Don't worry, we are here to help. Enter an IP address to look up its reputation."

<https://servicecentral.trendmicro.com/en-US/ers/>


Email Reputation

Tipos de listas de reputación:

- RBL
- QIL
- DUL



The screenshot displays the Trend Micro Email Reputation Services web interface. At the top, the Trend Micro logo and 'Email Reputation Services' are visible, along with a language dropdown set to 'English'. A navigation bar includes 'Dashboard' and 'IP Reputation'. The main content area is titled 'Lookup' and contains a form with the label 'Enter an IP address to look up its reputation.' The 'IP address:' field contains '179.162.150.79' and a red 'Check' button. Below the form, a 'Results' section shows the following information:

	IP:	179.162.150.79
	Reputation:	Unlisted in the spam sender list
	Listed in:	None
	Feedback:	Nominate this IP address to the global approved list

Areas de Almacenamiento

- **Quarantines** Almacena los correos “no deseados” definidos por política para ser enviados a cuarentena.
- **Deferred** Almacena los correos que no pueden ser enviados por algún motivo (problema de la propia Plataforma o del servidor que debe recibirlo).

TMES

Administración de la cuarentena

The screenshot displays the Trend Micro Email Security (TMES) Quarantine Query interface. The top navigation bar includes the Trend Micro logo, the product name "Trend Micro Email Security", and user information (UTC-03:00). The main navigation menu contains: Dashboard, Domains, Inbound Protection, Outbound Protection, Quarantine, Logs, Reports, Administration, and Help.

The current view is "Quarantine > Query". On the left, the "Criteria" section includes search filters for Period (Last 1 hour), Direction (Incoming), Recipient, Sender, Subject, Visibility (All), Reason (All), and Rule. A "Search" button is located at the bottom of this section.

The main content area shows a table with columns: Date, Sender, Recipient, Subject, Reason, and Rule. The table is currently empty, displaying "No data to display." Above the table are buttons for "Delete", "Deliver", and "Set Download Password". The table header also includes a checkbox and a "Records: 0 - 0 / 0" indicator with a "10" per page dropdown.

TMES

Configuración de la EUQ

The screenshot displays the Trend Micro Email Security (TMES) administration console. The breadcrumb trail is: Administration > End User Management > Logon Methods. The interface is divided into several sections:

- Sender Address Type:** A sidebar on the left allows selecting the type of sender address to filter by: Envelope address (selected), Message header, or Both. A "Save" button is visible below these options.
- Local Account Logon:** This section is titled "Local Account Logon" and includes a descriptive paragraph: "This method allows end users to log on to the End User Console with their user name and password. Enabling two-factor authentication adds an extra layer of security to the end user accounts." It contains three settings:
 - Local account logon: Enabled
 - Enforce two-factor authentication: Disabled
 - Source of managed accounts: A dropdown menu currently set to "Aliases synchronized from directories".
- Single Sign-On:** This section is titled "Single Sign-On" and includes a descriptive paragraph: "This method allows end users to log on to the End User Console with their existing corporate credentials through single sign-on (SSO)." It contains one setting:
 - Single sign-on: Disabled
- Table:** Below the Single Sign-On section is a table with columns: Profile, End User Console URL, Identity Provider, and Applied To. The table is currently empty, with a "No data to display" message at the bottom. "Add" and "Delete" buttons are located above and below the table.

Reporting - Email Security

TREND MICRO | Trend Micro Email Security

UTC-03:00 | [User Profile]

Dashboard | Domains | Inbound Protection | Outbound Protection | Quarantine | Logs | **Reports** | Administration | Help

Reports > My Reports

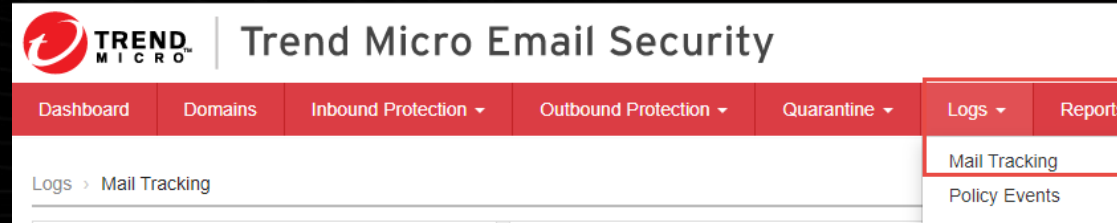
My Reports | Schedules

Type: All

Records: 1 - 10 / 24 | Page 1 / 3 | 10 per page

Period	Type	Report	Generated
04/02/2023 00:00:00 - 04/08/2023 23:59:59	Weekly		04/09/2023
03/26/2023 00:00:00 - 04/01/2023 23:59:59	Weekly		04/02/2023
03/01/2023 00:00:00 - 03/31/2023 23:59:59	Monthly		04/01/2023

Logs – Email Security

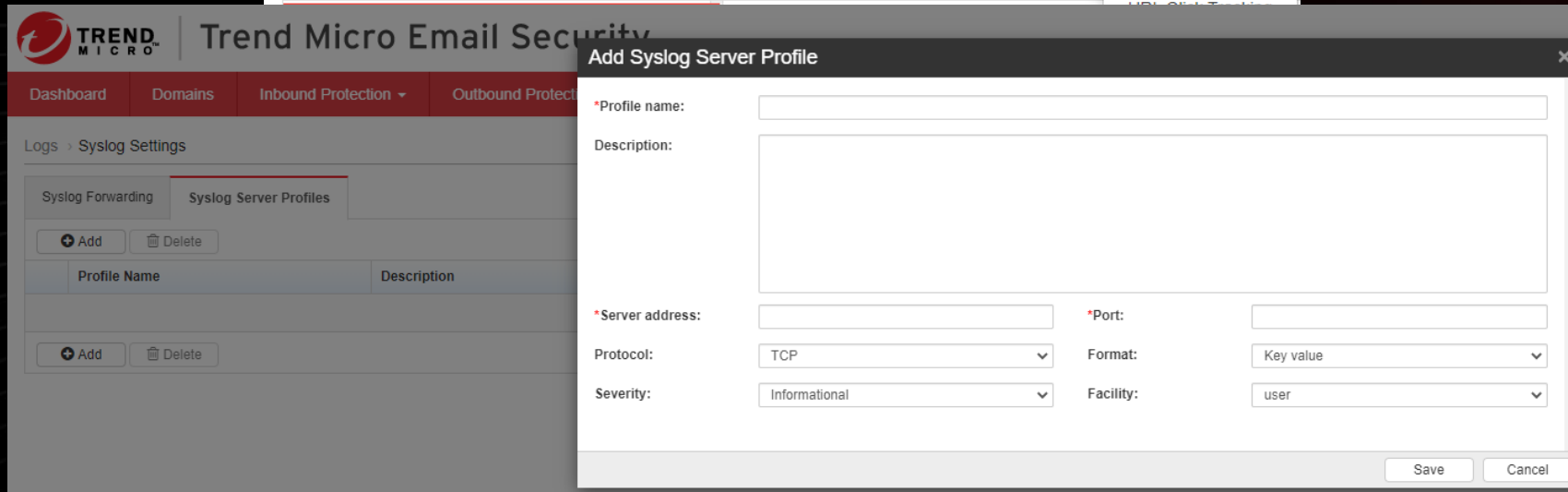


TREND MICRO | Trend Micro Email Security

Dashboard Domains Inbound Protection Outbound Protection Quarantine Logs Reports

Logs > Mail Tracking

- Mail Tracking
- Policy Events
- URL Classification



TREND MICRO | Trend Micro Email Security

Dashboard Domains Inbound Protection Outbound Protection

Logs > Syslog Settings

Syslog Forwarding Syslog Server Profiles

+ Add - Delete

Profile Name	Description
+ Add	- Delete

Add Syslog Server Profile

*Profile name:

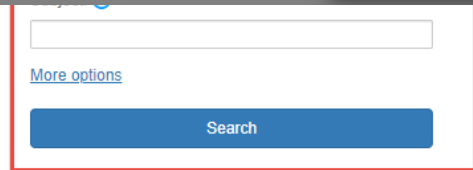
Description:

*Server address: *Port:

Protocol: TCP Format: Key value

Severity: Informational Facility: user

Save Cancel



[More options](#)

Search

Integración con Vision One

The screenshot displays the Trend Vision One™ Product Connector interface. A 'Connection Settings' dialog box is open, showing a list of products to connect. The main interface has a 'Connect' button and a table with columns: Product, Connection status, Data center, Identifier, and Description. A message states: 'No product has been connected yet. Click Connect to connect your first Trend Micro product.' A 'Connect Product' button is visible in the main interface.

Connection Settings

* Product:

- Trend Micro Email Security
- Trend Micro Apex One as a Service
- Trend Micro Cloud App Security
- Trend Micro Deep Discovery
- Trend Cloud One
- Trend Micro Deep Security Software
- TippingPoint Security Management System *Preview*
- Trend Micro Email Security *Preview***
- Trend Micro Web Security

Save Cancel

Trend Micro Email Solutions



Trend Micro Cloud App Security (CAS)

Capítulo 3

Protección avanzada con Trend Micro Cloud App Security

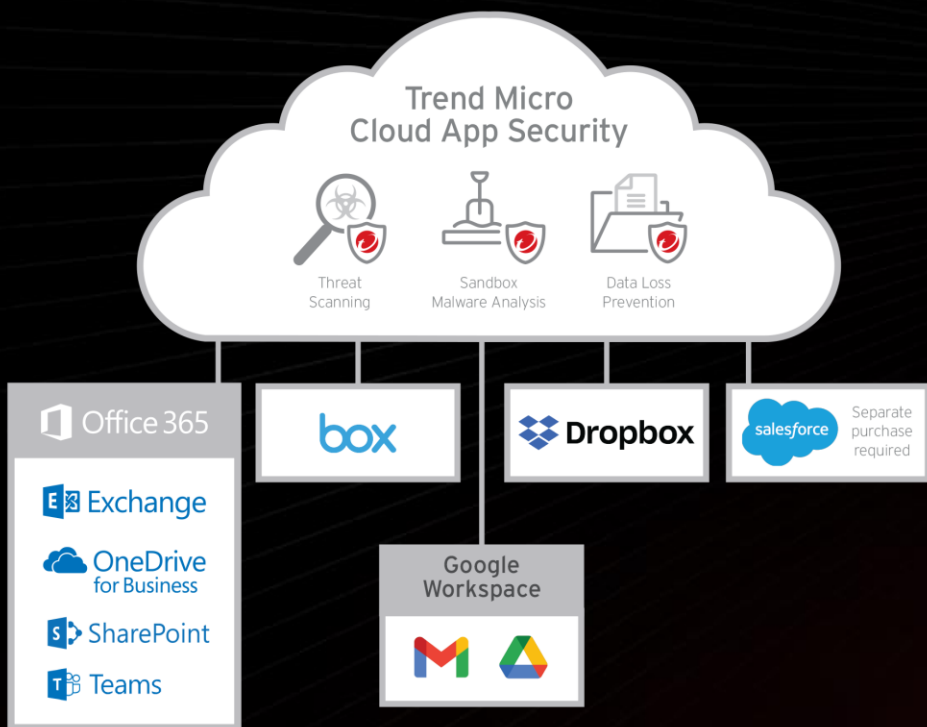
Seguridad práctica para Office 365



Cloud App Security Mail Service (API)

- Protección avanzada antiamenazas
 - Protección de email interna
 - Investigación / Remediación
 - OneDrive / SharePoint / Teams

Trend Micro Cloud App Security



Inteligente

- Encuentra amenazas avanzadas y zero-day con técnicas estáticas y dinámicas incluyendo sandboxing.
- Descubrimiento DLP, visibilidad y aplicación de políticas para servicios para compartir archivos en la nube.

Optimizado

- Integración directa nube a nube a través de la API.
- Protege email y archivos compartidos.

Conectado

- Administración centralizada de terminales, servidores y red de seguridad.
- Incluye Vision One XDR y parte de Managed XDR.

Microsoft 365

**Bloquea
amenazas
conocidas**



Firmas de
malware



Reputación
web y URL

Trend Micro Cloud App Security (CAS)

**Bloquea
amenazas
conocidas**



Firmas de
malware



Reputación
web y URL

**Detecta y bloquea
amenazas
desconocidas**



Detección
de exploit



Pre-execution
Machine
Learning



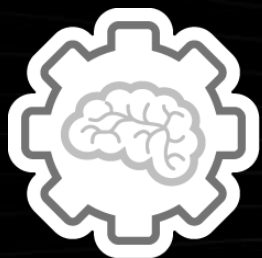
Análisis en
Sandbox



Machine
Learning para
phishing y BEC



Detección de malware desconocido



Pre-execution machine learning: Toma características claves para predecir si el archivo es malicioso. Mejora la eficiencia de la entrega de correos al encontrar malware desconocido antes del sandbox



Detección de exploit en documentos: analiza los archivos en búsqueda de exploits conocidos y posibles.



Análisis en Sandbox: análisis de comportamiento en varios SO en paralelo.

Detecte los ataques que ya están dentro de su organización

Disponible a través de la integración de servicios (CAS)

Inspecciona el correo electrónico interno en busca de amenazas avanzadas y fraude

Políticas granulares por grupo de AD

Acciones: etiquetar (advertencia), eliminar, poner en cuarentena



Respuesta y reparacion

Manual Scan For Advanced Threat Protection

Selected Policy for Manual Scan

Policy Name	Type	Targets	Rules	Scan Details
Exchange Policy for Executives	Exchange Online	Executives		Estimated time required: 6 minutes

Showing 1 to 1 of 1 entries

Scan Type

Scan and protect
 Scan only

Scope:

Scan recently: day(s)
 Scan between: and

Report Recipients

Separate multiple email addresses with a semicolon

Note Manual scan does not include Virtual Analyzer scanning.

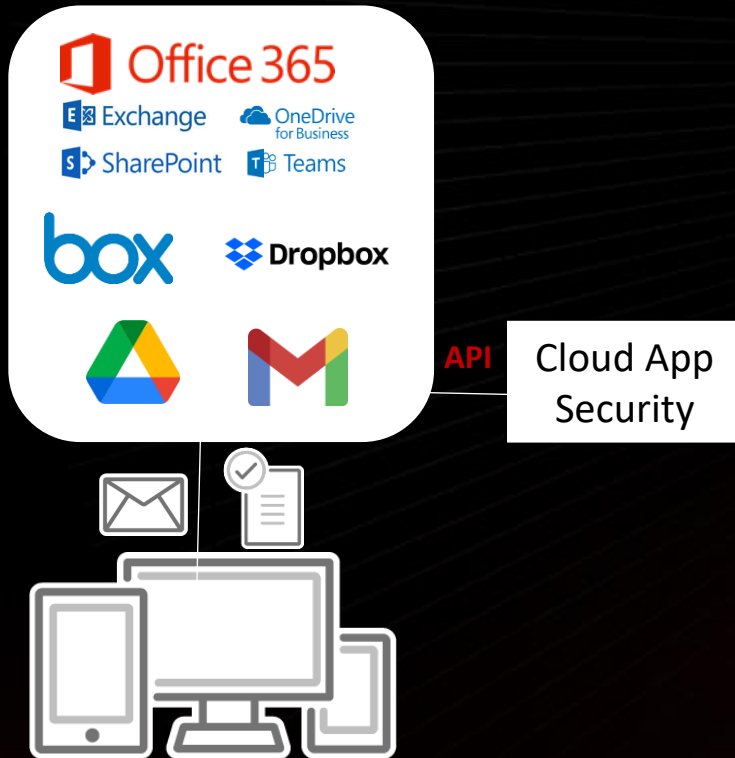
La importancia del escaneo manual que se realiza en tiempo real.

Microsoft Teams Protection



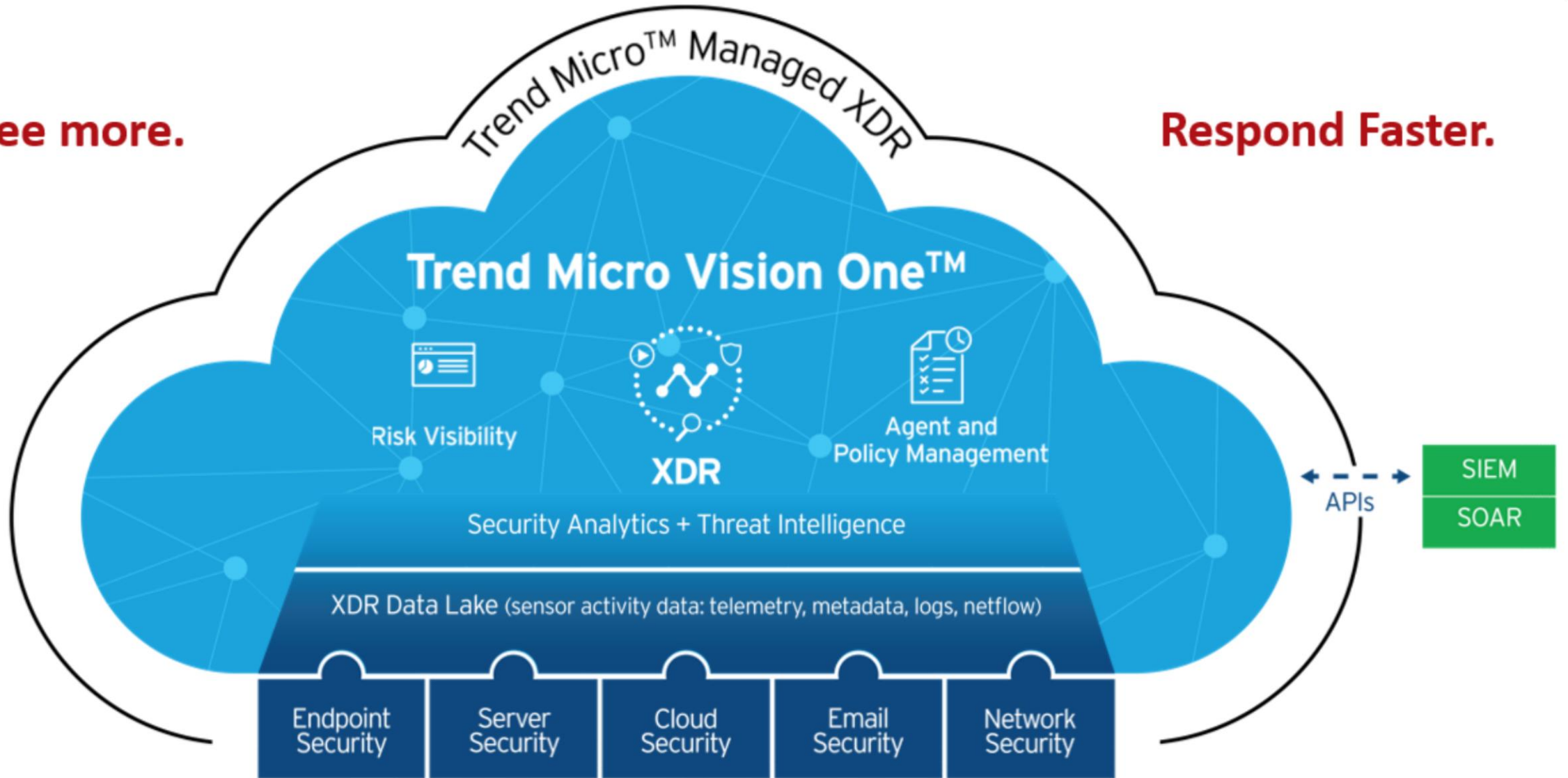
- Protege el "Chat" y "Teams" de Microsoft Teams para los archivos y datos sensibles enviados en los mensajes de chat o compartidos en los canales de Teams
 - Protección contra amenazas avanzadas en tiempo real
 - DLP

Integración sencilla con los servicios SaaS



See more.

Respond Faster.



Por qué añadir XDR al correo electrónico

Malware Infection Source



Datos de la actividad :

- Metadatos de los mensajes (correo electrónico externo + interno))
- Metadatos adjuntos
- Enlaces externos
- Actividad de los usuarios (logins)

Detectar: ¿Hay cuentas comprometidas que envían correos electrónicos internos de phishing?

Investiga: ¿Quién más ha recibido este correo electrónico/amenaza?

Responder: Poner en cuarentena el correo electrónico, eliminar el correo electrónico, bloquear el remitente, bloquear URLs/archivos

Service Account Integration

Administration > Service Account

← Previous **1** Next →

	Account Name / Registration Token	Service Type	Expiration Date	Status
<input type="checkbox"/>	tmcasex_...onmicrosoft.com	Exchange Online	N/A	[Migration Available] [Change Password]
<input type="checkbox"/>	tmcassp_...onmicrosoft.com	SharePoint Online	N/A	[Change Password]


- Service:** Exchange Online OneDrive for Business SharePoint Online Microsoft Teams Gmail Google Drive Box Dropbox Salesforce Sandbox [Preview](#)

Policy Configuration


Priority	Policy	Targets	Rules
Exchange Online Policies Blocked Lists for Exchange Online enabled !			
<input type="checkbox"/>	ON Exchange Policy	All Users	AS WR VA
1			
<input type="checkbox"/>	OFF Default Exchange Policy ATP DEFAULT POLICY: Policy used if no other policy created for target	All Users	AS WR VA
2			
OneDrive for Business Policies			
<input type="checkbox"/>	ON OneDrive Policy DEFAULT POLICY: Policy used if no other policy created for target	All Users	WR VA
1			
SharePoint Online Policies			
<input type="checkbox"/>	ON Sharepoint Policy DEFAULT POLICY: Policy used if no other policy created for target	All Sites	WR VA
1			

Showing 1 to 4 of 4 entries

Trend Micro Cloud App Security technologies:



Anti-malware engine



Web reputation technology




Sandbox technology



Pre-execution machine learning technology



Anti-phishing technology using machine learning



Anti-BEC technology using machine learning

Quarantine

TREND MICRO Cloud App Security

Dashboard Advanced Threat Protection Data Loss Prevention Logs **Quarantine**

Search [] Select Date Range [] Search

Showing: 100 / 15220 items

Restore Download Delete

Timestamp	Security Filter	Security Risk Name	Status	Affected User	File Name
✓ Sep 17, 2020 12:00:36	Malware Scanning	Eicar_test_file	Quarantined	instantdemo@productcloud.me	MsgBody
✓ Sep 17, 2020 12:00:24	Web Reputation	Spyware: [http://][/]wrs21[.]wins...	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 12:00:24	Malware Scanning	Ransom_BLOCCATO.SM	Quarantined	instantdemo@productcloud.me	invoice.exe
✓ Sep 17, 2020 12:00:23	Web Reputation	Spyware: [http://][/]wrs21[.]wins...	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 12:00:20	Advanced Spam Protection	Phishing	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 12:00:16	Advanced Spam Protection	Phishing	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 12:00:16	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 12:00:15	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:51	Advanced Spam Protection	Phishing	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:31	Web Reputation	Spyware: [http://][/]wrs21[.]wins...	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:26	Malware Scanning	Eicar_test_file	Quarantined	instantdemo@productcloud.me	MsgBody
✓ Sep 17, 2020 11:45:21	Malware Scanning	Ransom_BLOCCATO.SM	Quarantined	instantdemo@productcloud.me	invoice.exe
✓ Sep 17, 2020 11:45:18	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:15	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:14	Advanced Spam Protection	Phishing	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:45:14	Web Reputation	Spyware: [http://][/]wrs21[.]wins...	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:00:16	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:00:16	Advanced Spam Protection	BEC	Quarantined	instantdemo@productcloud.me	Mail Body
✓ Sep 17, 2020 11:00:13	Malware Scanning	Ransom_BLOCCATO.SM	Quarantined	instantdemo@productcloud.me	invoice.exe

Automatically delete quarantined items older than 30 day(s)

Service: Exchange Online

Security Filter: Exchange Online (7961), OneDrive for Business (3992), SharePoint Online (3267), Dropbox

Affected User: instantdemo@productcloud.me (15220)

Status: Quarantined (15087), DeleteFailure (133)

Logs & Reporting

TREND MICRO Cloud App Security (7) (2) Welcome demo

Dashboard Advanced Threat Protection Data Loss Prevention **Logs** Quarantine

Templates Reports Scheduled Report

Search Select Date Range Search

Save... Export... Preview Report Showing: 100 / 1076 items

Timestamp	User	Action	Details
Sep 15, 2020 03:30:30	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 15, 2020 02:39:21	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 15, 2020 00:46:34	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 15, 2020 00:34:04	Cloud App Security	DROPBOX_SCHEDULED_SYNC	Success
Sep 15, 2020 00:04:32	Cloud App Security	ONEDRIVE_SCHEDULED_SYNC	Success
Sep 14, 2020 23:21:58	Cloud App Security	EXCHANGE_SCHEDULED_SYNC	Success
Sep 14, 2020 22:34:24	Cloud App Security	SHAREPOINT_SCHEDULED_SYNC	Success
Sep 14, 2020 15:35:16	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 15:34:25	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 11:46:53	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 08:36:27	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 06:35:56	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 05:26:24	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 03:44:40	productcloudcas@gmail.com	LOGON	productcloudcas@gmail.com
Sep 14, 2020 00:34:03	Cloud App Security	DROPBOX_SCHEDULED_SYNC	Success
Sep 14, 2020 00:15:45	Cloud App Security	EXCHANGE_SCHEDULED_SYNC	Success
Sep 14, 2020 00:05:58	Cloud App Security	ONEDRIVE_SCHEDULED_SYNC	Success

Type Audit Logs

- Security Risk Scan
- Ransomware
- Virtual Analyzer
- Data Loss Prevention
- Quarantine
- Audit Logs
- API Integration

- LOGON 655
- DROPBOX_SCHEDULED_SYNC 91
- EXCHANGE_SCHEDULED_SYNC 90
- ONEDRIVE_SCHEDULED_SYNC 90
- SHAREPOINT_SCHEDULED_SYNC 90
- CONNECT_TO_XDR 50
- UPDATE_POLICY 7
- ADD_AUTOMATION_API_AUTHENTICATIO... 1
- DISCONNECT_FROM_XDR 1



DEMOS

Actividad:

Reconocimiento de Phishing

<https://phishingquiz.withgoogle.com/>

¡Muchas Gracias!

