



Email solutions
Trend Micro

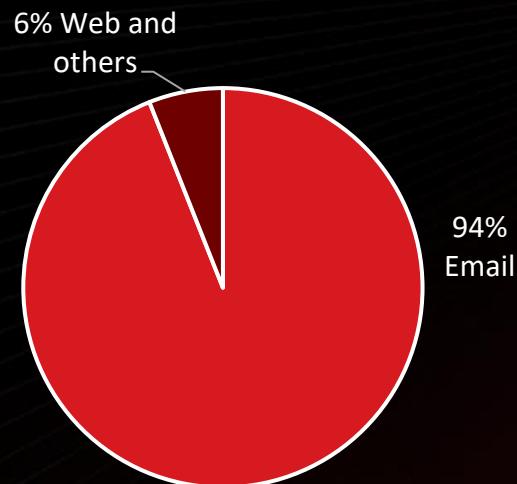


Objetivos del Curso

- 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.

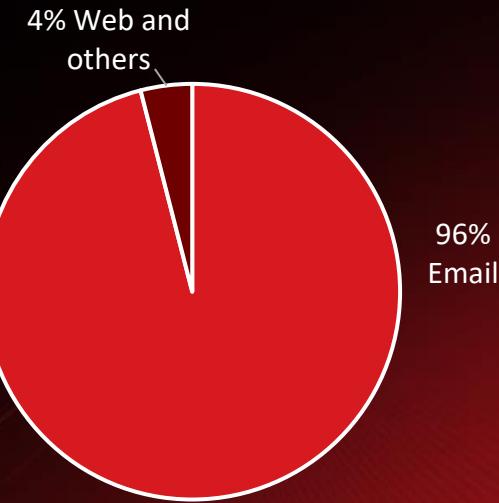
La mayoría de los ciberataques provienen del **correo electrónico**

Malware Delivery Method



Source: Verizon DBIR 2019

Social Engineering Attack Delivery Method



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



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

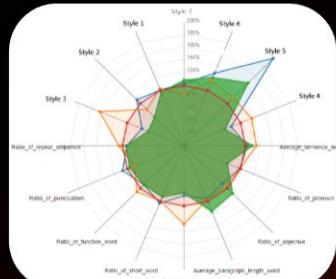
Behavior + Intention analysis

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

Mimics the decision making of a security expert



Authorship analysis

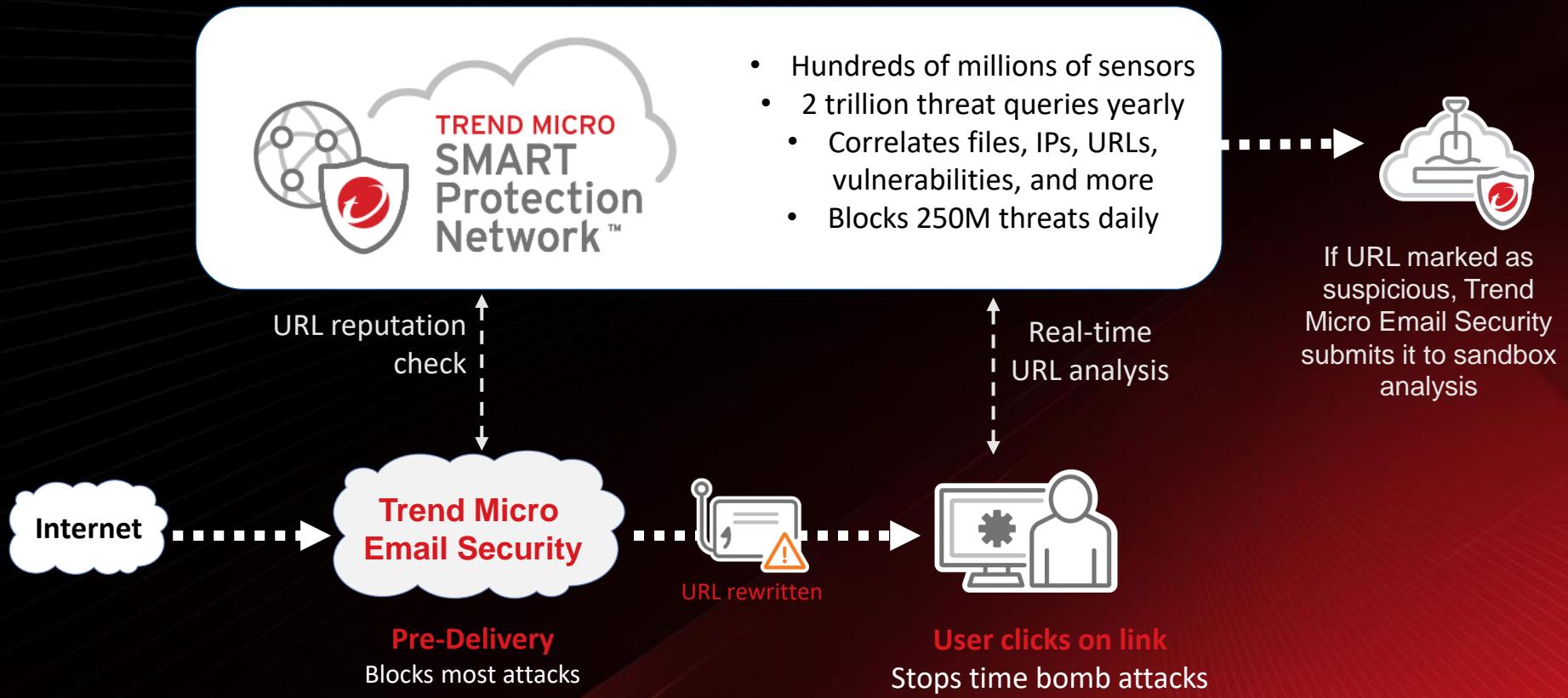


Compares a suspected impersonation to AI model of high-profile user's writing style

WRITING STYLE DNA

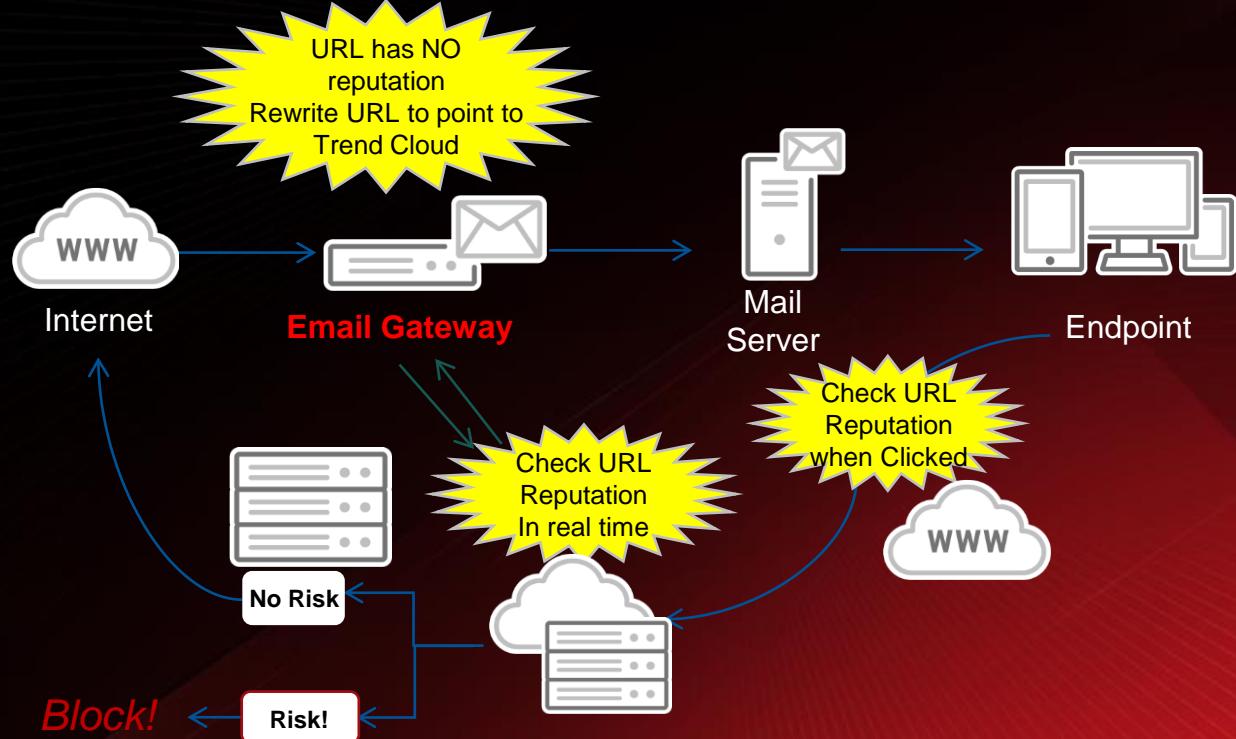


Malicious URL Protection



Threat detection – URL Time Of Click

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

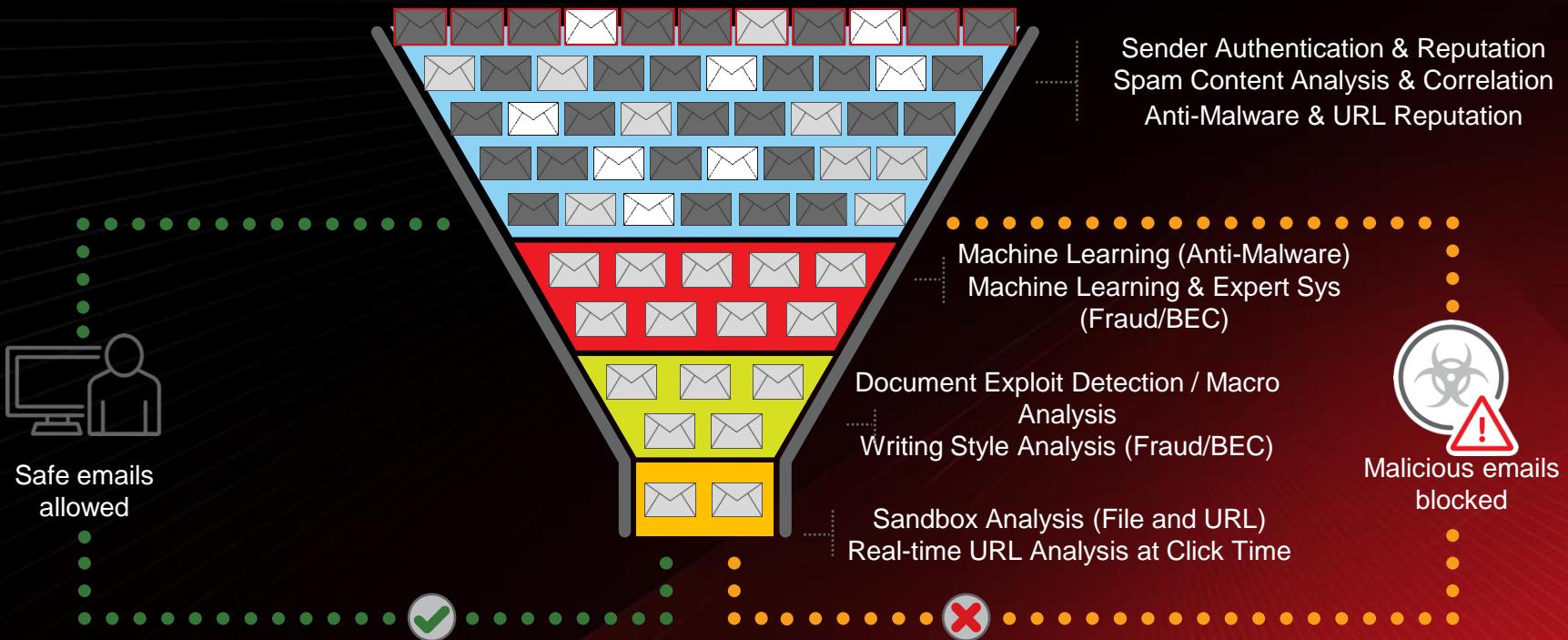




SMART: Unique Blend to Protect Email

LEGEND

Known Good	Known Bad	Unknown
------------	-----------	---------



Trend Micro Email Security Portfolio



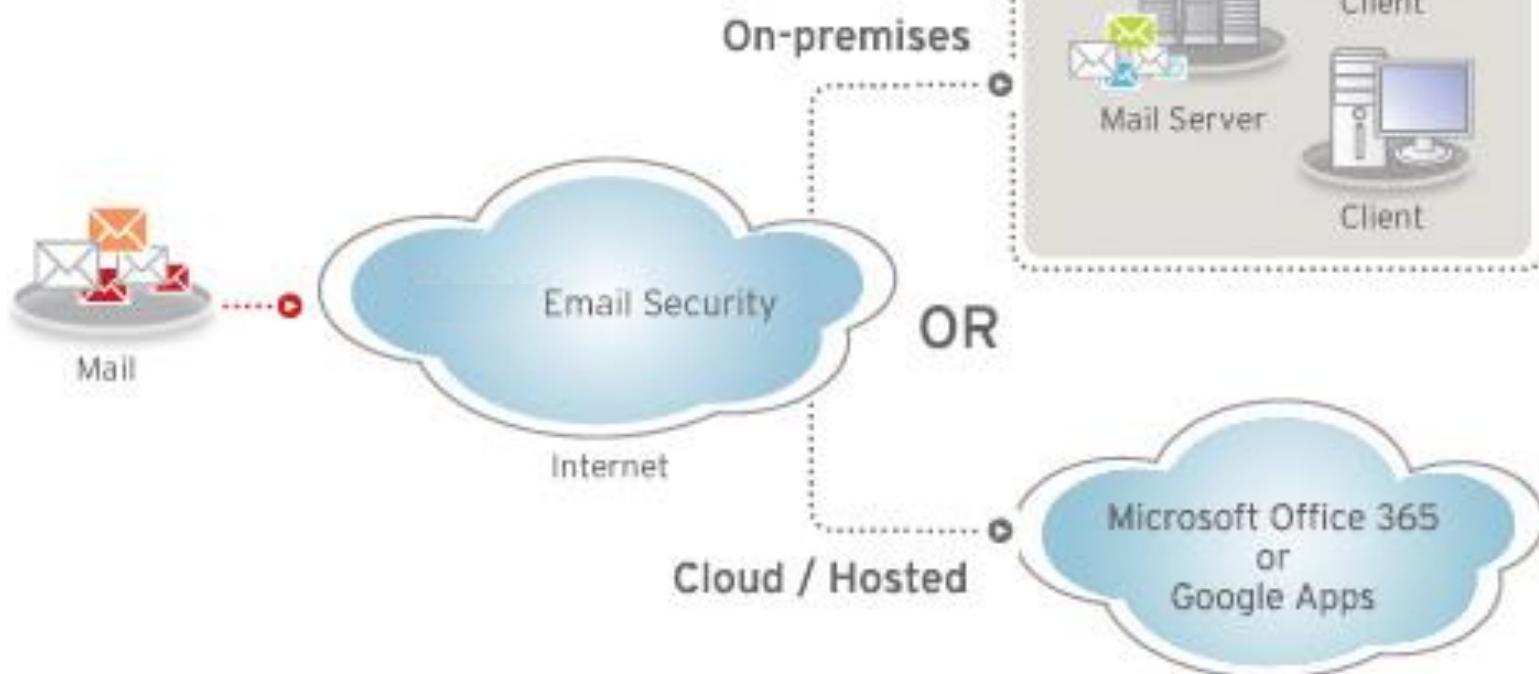
Trend Micro Email Solutions



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 [i](#)

* @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**. [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**. [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 website. At the top left is the Trend Micro logo. Next to it, the text "Trend Micro Email Security" is displayed. Below this, a large image of a woman with long brown hair, wearing a white shirt, looking towards the camera. To her left, there is promotional text: "Stop advanced email threats and spam before they reach your network" and a description of the product's capabilities. A blue "Learn more" button is located below the promotional text. On the right side of the page is a "Log On" form. It contains two input fields: one for "Type user name" and another for "Type password". Below these fields is a red "Log On" button. At the bottom of the form is a link "Forgot your password?". At the very bottom of the page, there is a footer with links: "© 2023 Trend Micro Incorporated.", "Legal Policies & Privacy", "Contact Us", and "Trend Micro Home". To the right of these links is the Trend Micro logo.

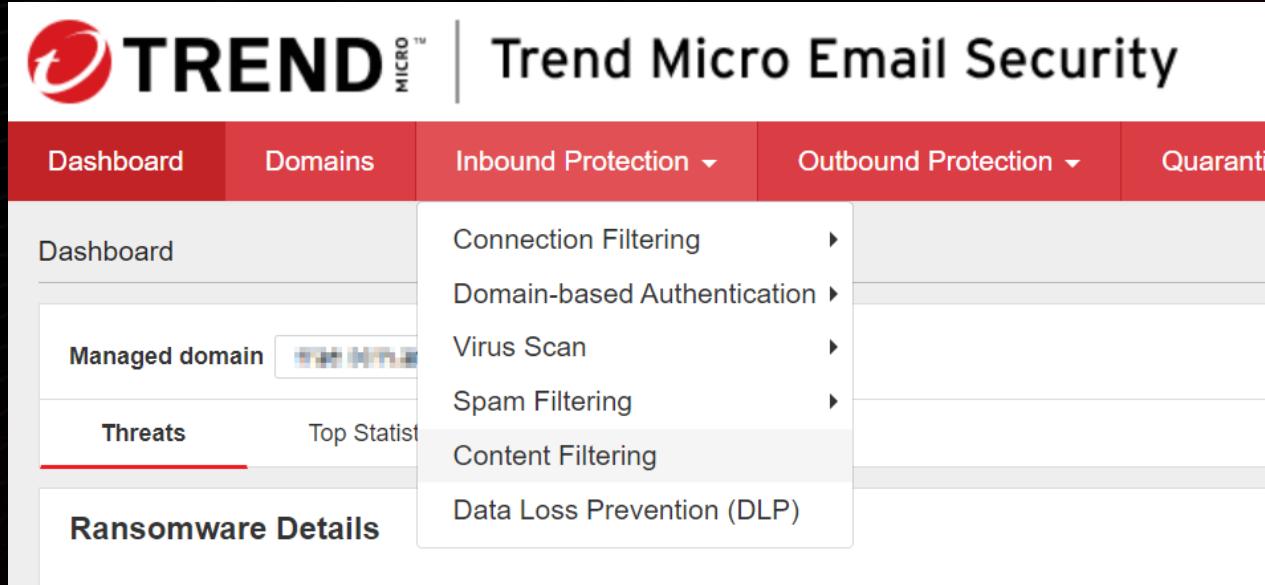
URL de Ingreso:

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 cheques aplicables sobre ambas plataformas:

- SPF

- DKIM

- DMARC

The screenshot shows the Trend Micro Email Security interface. At the top, there's a navigation bar with links for Dashboard, Domains, Inbound Protection, Outbound Protection, Quarantine, Logs, Reports, and Administration. The 'Domains' link is currently selected, highlighted in red. Below the navigation bar, there's a sidebar with sections for Dashboard, Managed domain, Threats (which is underlined in red), and Top Statistics. A 'Ransomware Details' section is also present. The main content area has a 'Connection Filtering' dropdown expanded, showing options like Sender IP Match, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) Verification, and Domain-based Message Authentication, Reporting and Conformance (DMARC). Other sections visible include 'Domain-based Authentication', '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, there's a navigation bar with the Trend Micro logo, the text "Email Reputation Service", a globe icon, and a "Sign In" button. Below the navigation is a red header bar with links for "Home", "IP Reputation", and "More Info". The main content area has a white background. On the left, there's a sidebar with buttons for "Lookup", "Add to Global Approved List", and "Add to Global Blocked List". To the right of the sidebar, the text "Worried about being spammed?" is displayed, followed by "Don't worry, we are here to help." and "Enter an IP address to look up its reputation.". Below this text is a search input field containing "Ex. 127.0.0.1" and a "Look Up" button.

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

Email Reputation

Tipos de listas de reputación:

- RBL

- QIL

- DUL

The screenshot shows the Trend Micro Email Reputation Services interface. At the top, there is a navigation bar with the Trend Micro logo, the service name "Email Reputation Services", a language selector set to "English", and a help icon. Below the navigation bar, there are two tabs: "Dashboard" and "IP Reputation". The "IP Reputation" tab is selected. The main area is titled "Lookup" and contains a form where the IP address "179.162.150.79" has been entered into the "IP address:" field, and a "Check" button is visible. Below the form, under the heading "Results", is a table with the following data:

	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 recibirla).

TMES

Administración de la cuarentena

 **TREND** MICRO™ | Trend Micro Email Security

UTC-03:00 | 

Dashboard Domains Inbound Protection Outbound Protection Quarantine Logs Reports Administration Help

Quarantine > Query

Criteria

Period: Last 1 hour

Direction: Incoming

Recipient:

Sender:

Subject:

Visibility: All

Reason: All

Rule:

Delete Deliver Set Download Password

Records: 0 - 0 / 0 | 10 per page

No data to display.

Delete Deliver

Records: 0 - 0 / 0 | 10 per page

TMES

Configuración de la EUQ

The screenshot shows the TMES web interface with the following details:

- Header:** Trend Micro Email Security
- Breadcrumbs:** Quarantine > End User Management > Logon Methods
- Left Sidebar:** Sender Address Type (radio buttons: Envelope address, Message header, Both). Buttons: Save, Cancel.
- Local Account Logon:** Describes the method allowing end users to log on with their user name and password. It includes:
 - Local account logon: Enabled (switch is on)
 - Enforce two-factor authentication: Disabled (switch is off)
 - Source of managed accounts: Aliases synchronized from directories
- Single Sign-On:** Describes the method allowing end users to log on through single sign-on (SSO). It includes:
 - Single sign-on: Disabled (switch is off)
- Table:** A table for managing profiles. Headers: Profile, End User Console URL, Identity Provider, Applied To. Sub-headers: Add, Delete. Body: No data to display.

Reporting - Email Security

TREND MICRO™ Trend Micro Email Security

UTC-03:00 | [REDACTED]

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

The screenshot shows the Trend Micro Email Security web interface. At the top, there's a navigation bar with links for Dashboard, Domains, Inbound Protection, Outbound Protection, Quarantine, Logs (which is currently selected), Reports, Mail Tracking, Policy Events, and Help & Support. Below the navigation, a breadcrumb trail indicates the user is in the Logs > Mail Tracking section.

The main content area displays a sub-menu for 'Logs' with options for Syslog Settings, Syslog Forwarding, and Syslog Server Profiles. Under 'Syslog Server Profiles', there are buttons for '+ Add' and 'Delete'. A table lists existing profiles with columns for 'Profile Name' and 'Description'. Below the table are buttons for '+ Add' and 'Delete'.

A modal dialog titled 'Add Syslog Server Profile' is open in the center. It contains fields for 'Profile name' (with a required asterisk), 'Description', 'Server address' (with a required asterisk), 'Protocol' (set to TCP), 'Port' (empty), 'Format' (set to Key value), 'Severity' (set to Informational), and 'Facility' (set to user). At the bottom of the dialog are 'Save' and 'Cancel' buttons.

At the bottom of the page, there's a search bar with a red border and a 'Search' button, along with a link to 'More options'.

Integración con Vision One

The screenshot shows the Trend Vision One™ Product Connector interface. On the left is a vertical toolbar with icons for various products: Cloud App Security, Deep Discovery, Cloud One, Deep Security, TippingPoint, Email Security (selected), and Web Security. The main area displays a table with columns: Product, Connection status, Data center, Identifier, and Description. A message at the top states, "No product has been connected yet. Click Connect to connect your first Trend Micro product." A prominent blue "Connect" button is located at the top left of the main area. Below it is a "Connect Product" button. To the right, a modal window titled "Connection Settings" is open, showing a dropdown menu for "Product" with several options listed: Trend Micro Email Security (selected), 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 (selected), and Trend Micro Web Security. At the bottom of the modal are "Save" and "Cancel" buttons.

Trend Vision One™ | Product Connector

Connect

Product Connection status Data center Identifier Description

No product has been connected yet. Click Connect to connect your first Trend Micro product.

Connect Product

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

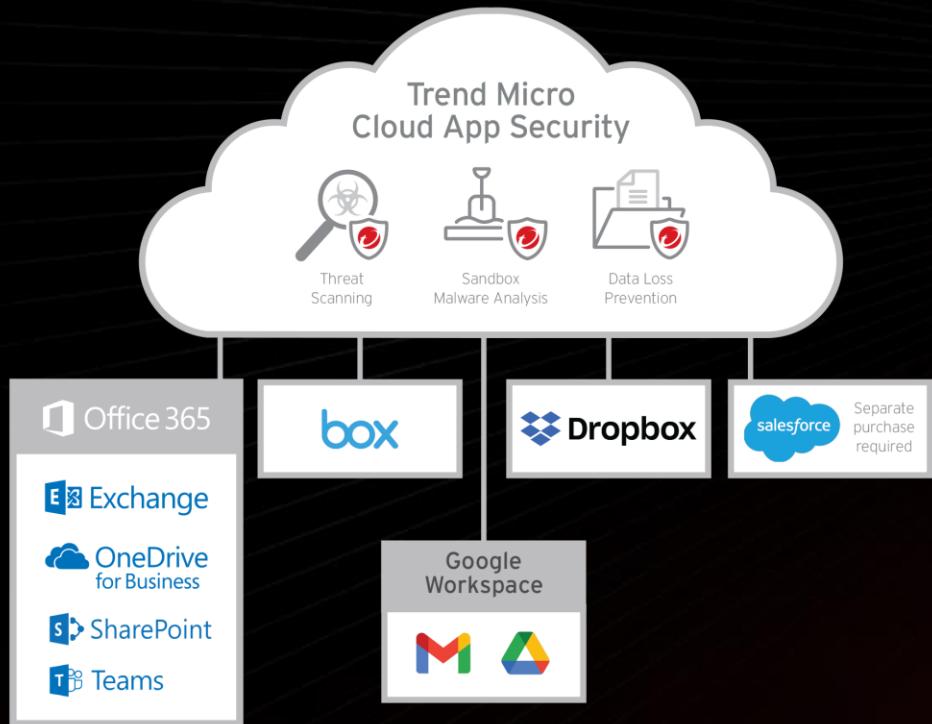
Seguridad práctica para Office 365



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



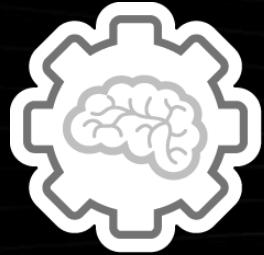
Análisis en Sandbox



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



Empleado A

*dispositivo o credenciales de correo
electrónico comprometidos*



Malware/Fraud



Empleado B

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	AS Q E WR VA	<i>Estimated time required: 6 minutes</i>

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.

Scan Now **Cancel**

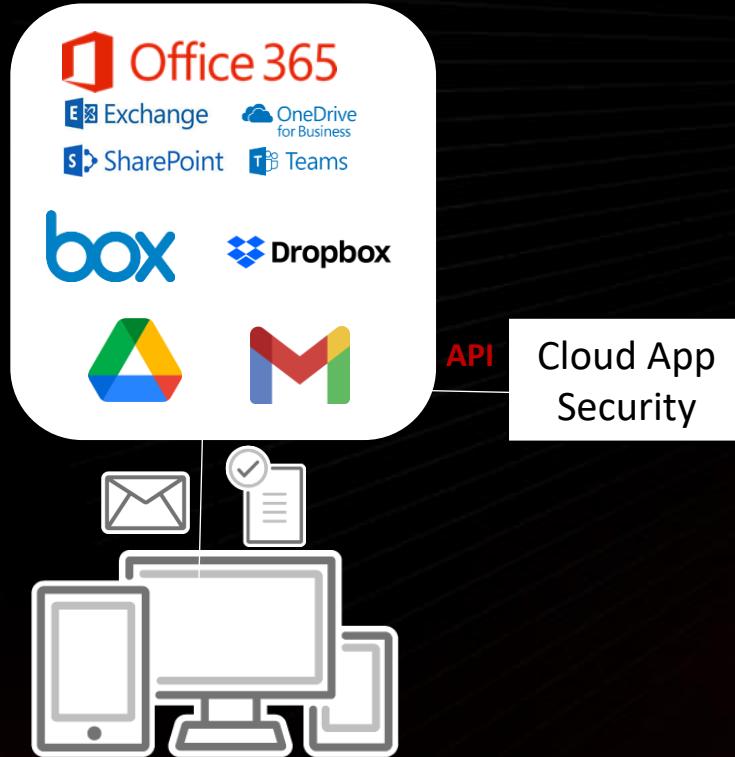
La importancia del escaneo manual que se realiza en tiempo real.

Microsoft Teams Protection



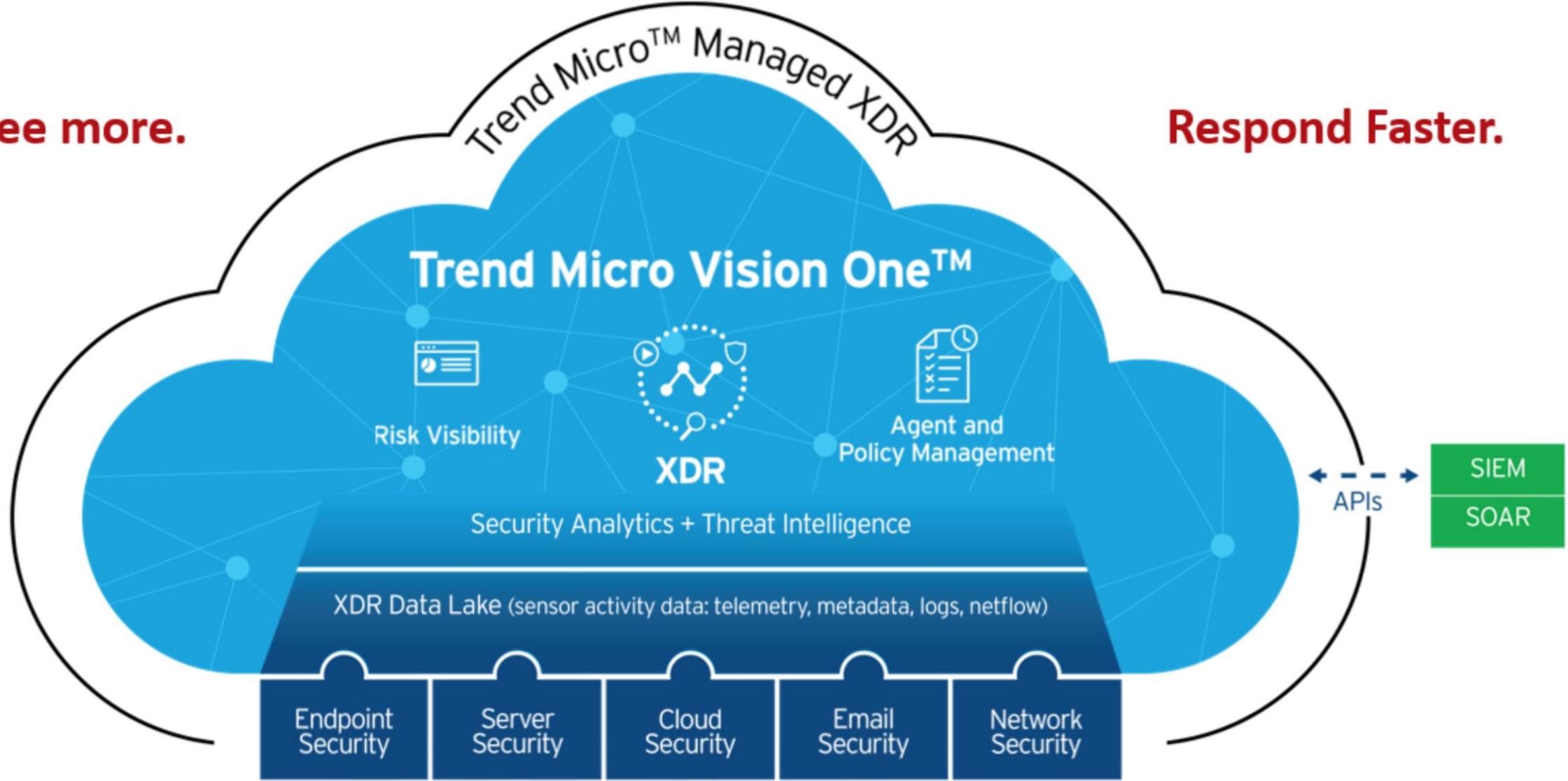
- Protege el "Chat" y "Teams" de Microsoft Teams para los archivos y datos sensibles enviados en los mensajes de chat o compartidos en los canales de Teams
 - Protección contra amenazas avanzadas en tiempo real
 - DLP

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

		Add	Remove	← Previous	1	Next →	Search:
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 !				
1	<input type="checkbox"/> ON <input type="checkbox"/> Exchange Policy		All Users	
2	<input type="checkbox"/> OFF Default Exchange Policy ATP	DEFAULT POLICY: Policy used if no other policy created for target	All Users	
OneDrive for Business Policies				
1	<input type="checkbox"/> ON <input type="checkbox"/> OneDrive Policy	DEFAULT POLICY: Policy used if no other policy created for target	All Users	
SharePoint Online Policies				
1	<input type="checkbox"/> ON <input type="checkbox"/> Sharepoint Policy	DEFAULT POLICY: Policy used if no other policy created for target	All Sites	
Showing 1 to 4 of 4 entries				
← Previous 1 Next →				



Quarantine

TREND MICRO Cloud App Security

Dashboard Advanced Threat Protection Data Loss Prevention Logs Quarantine

Service: Exchange Online

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

Affected User: instantdemo@productcloud.me (15220)

Status: Quarantined (15087), DeleteFailure (133)

Search: Select Date Range, Search

Showing: 100 / 15220 items

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 days

Logs & Reporting

The screenshot shows the Trend Micro Cloud App Security interface with the 'Logs' tab selected. On the left, there's a sidebar with 'Templates', 'Reports', and 'Scheduled Report' buttons. Below them is a dropdown menu for 'Type' set to 'Audit Logs', showing various log categories with counts: Security Risk Scan (645), Ransomware, Virtual Analyzer, Data Loss Prevention (51), Quarantine (19), 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_AUTHENTICATION (1), and DISCONNECT_FROM_XDR (1). The main area displays a table of logs with columns for 'Timestamp', 'User', 'Action', and 'Details'. The table shows 100 items out of 1076. The first few rows include entries like 'Sep 15, 2020 03:30:30 productcloudcas@gmail.com LOGON', 'Sep 15, 2020 02:39:21 productcloudcas@gmail.com LOGON', and 'Sep 15, 2020 00:46:34 productcloudcas@gmail.com LOGON'. Most actions listed are 'Success'.

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



DEMONSTRATIONS

Actividad:
Reconocimiento de Phishing

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

¡Muchas Gracias!

