



Email solutions
Trend Micro

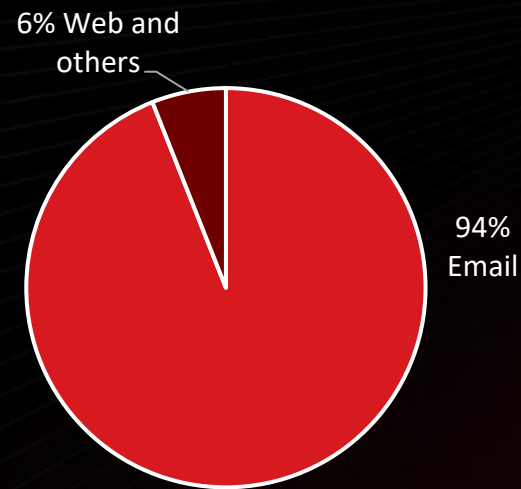


Objetivos del Curso

- 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.

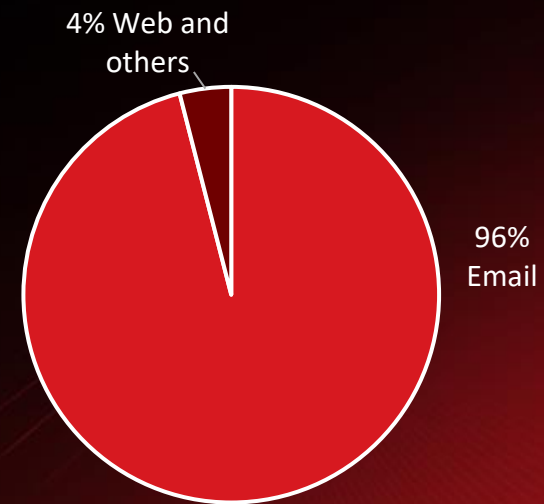
La mayoría de los ciberataques provienen del correo electrónico

Malware Delivery Method



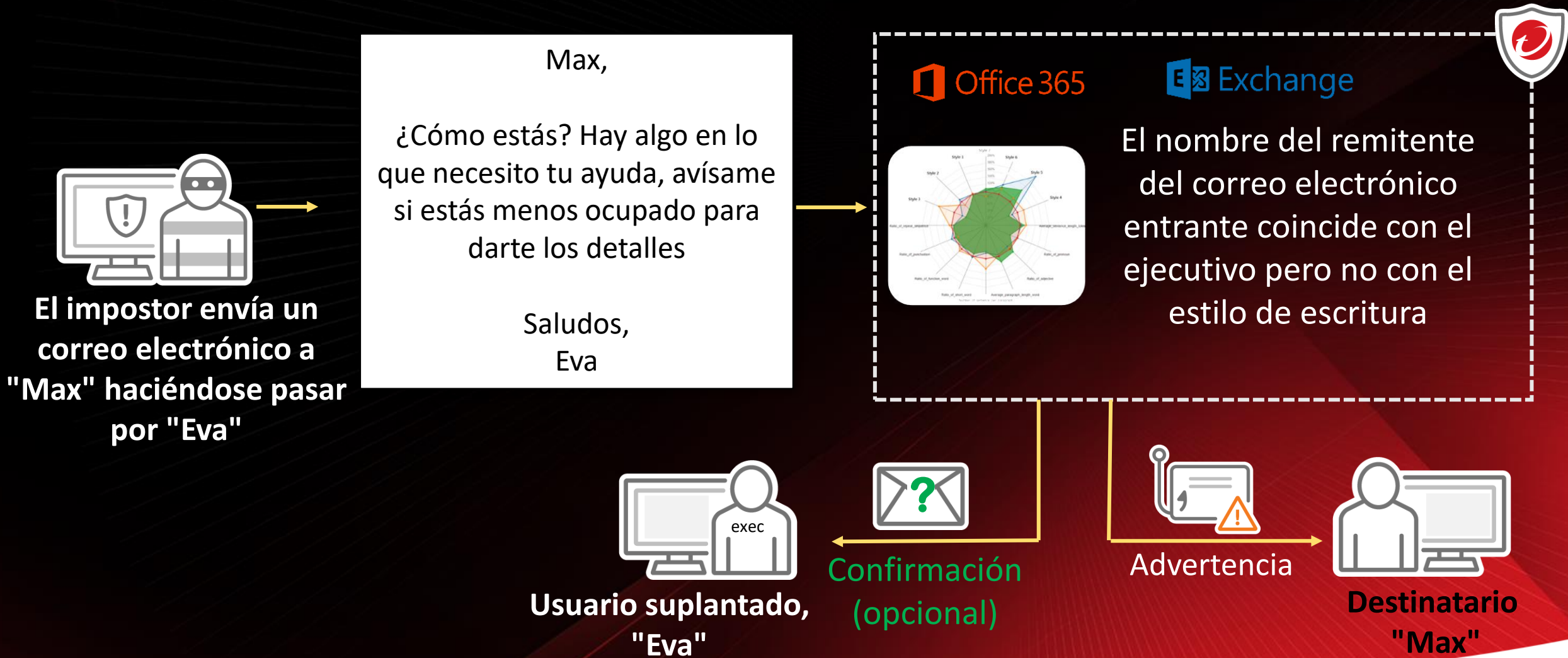
Source: Verizon DBIR 2019

Social Engineering Attack Delivery Method



Source: Verizon DBIR 2020

Business Email Compromise (BEC) Attacks

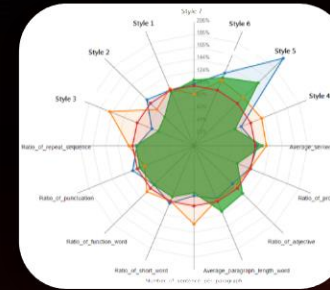


AI based BEC Detection

Behavior + Intention analysis

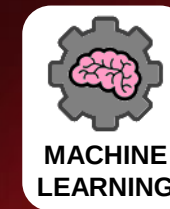
Behavior	Routing behavior
	Cousin domain
	High-profile user similarity
	...
Intention	Financial impact
	Urgency
	...

Mimics the
decision making
of a security
expert

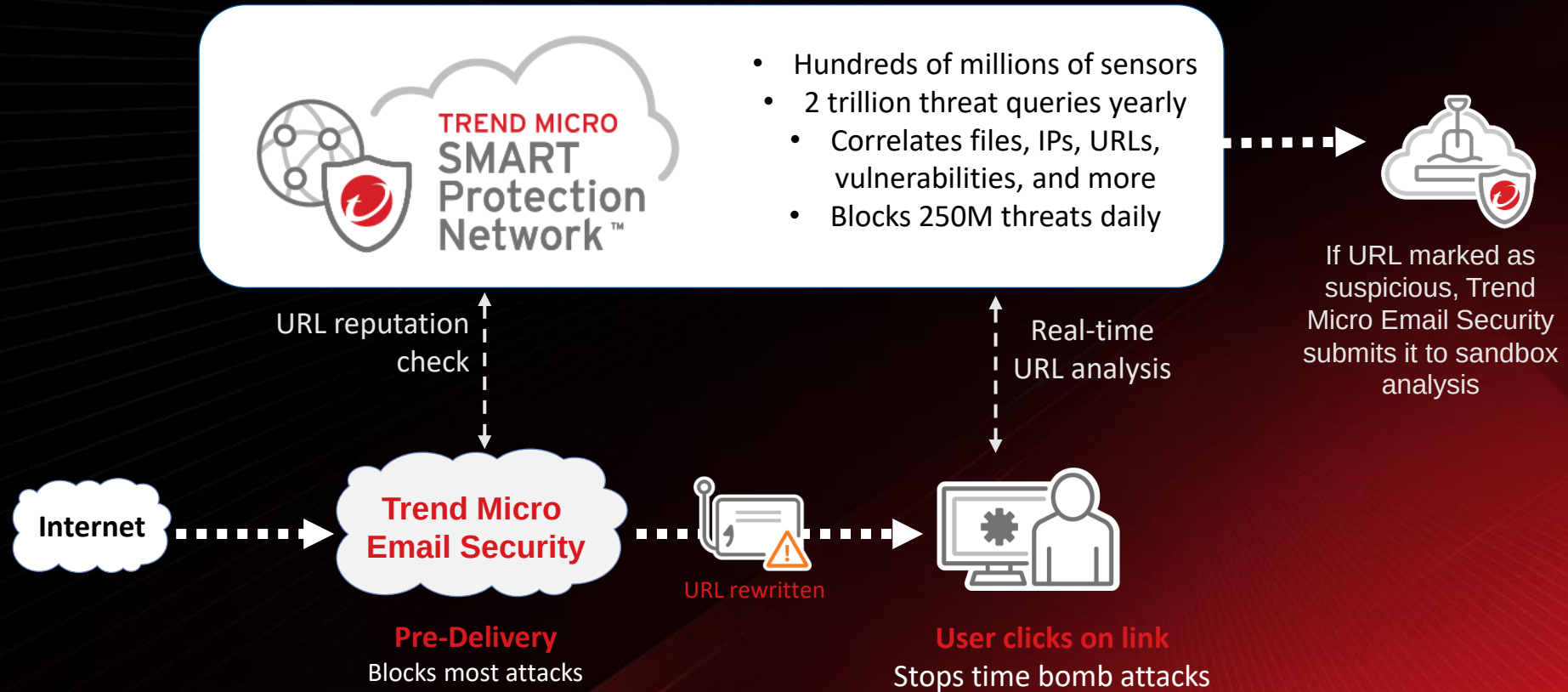


Compares a suspected impersonation to AI model of high-profile user's writing style

WRITING STYLE DNA

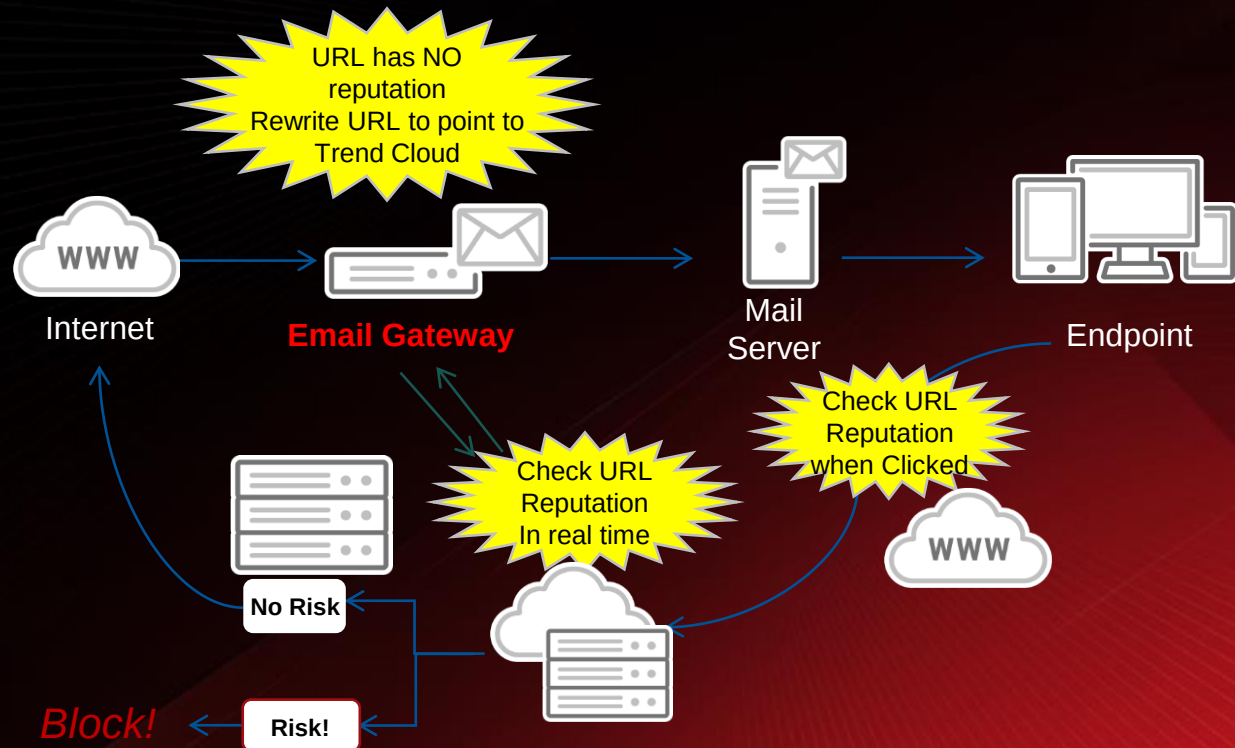


Malicious URL Protection



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



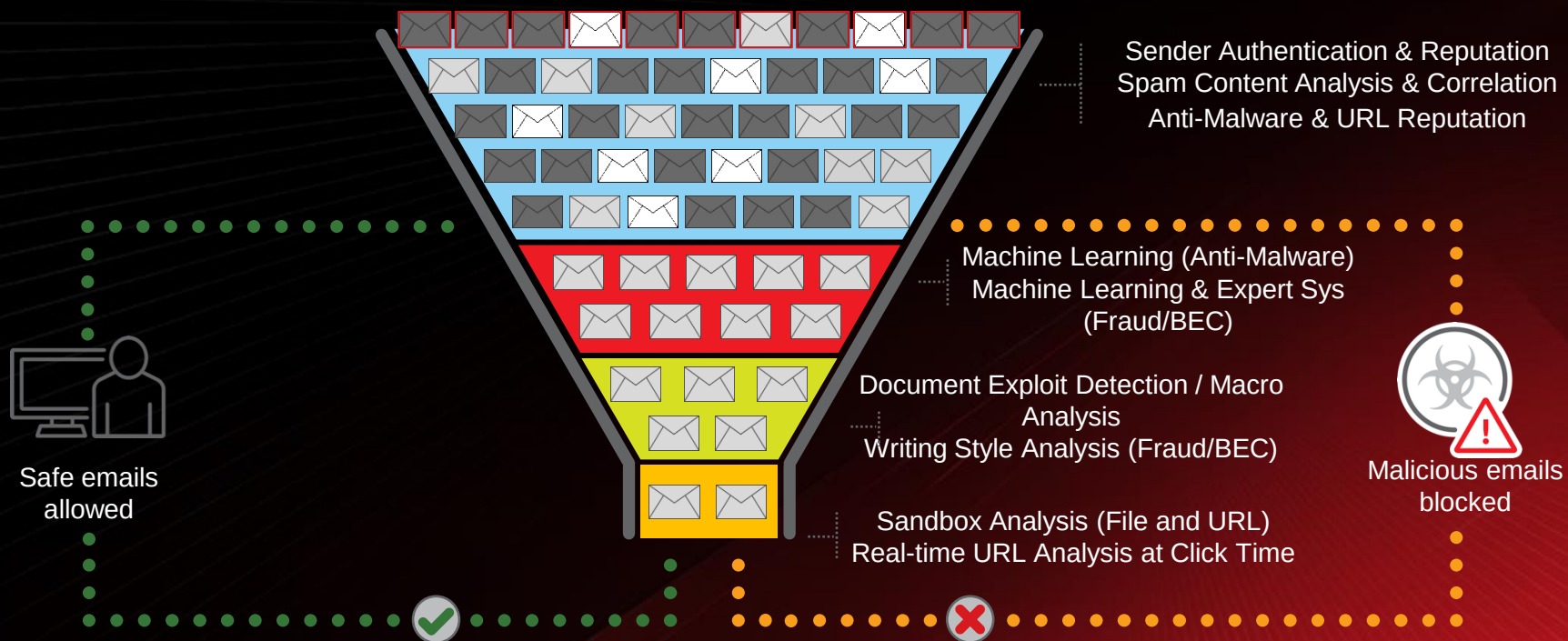
Known Good



Known Bad



Unknown



Trend Micro Email Security Portfolio



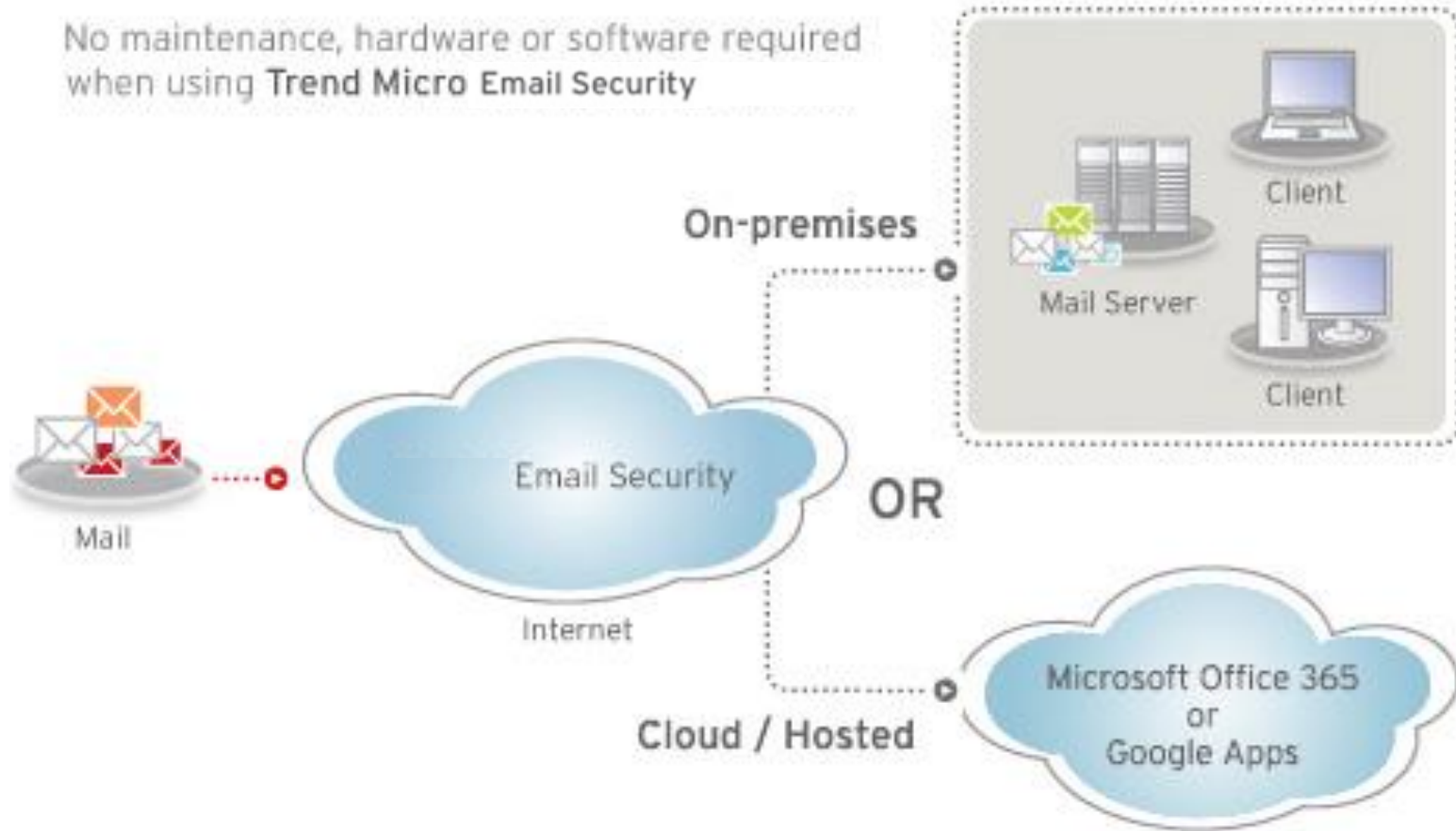
Trend Micro Email Solutions



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

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

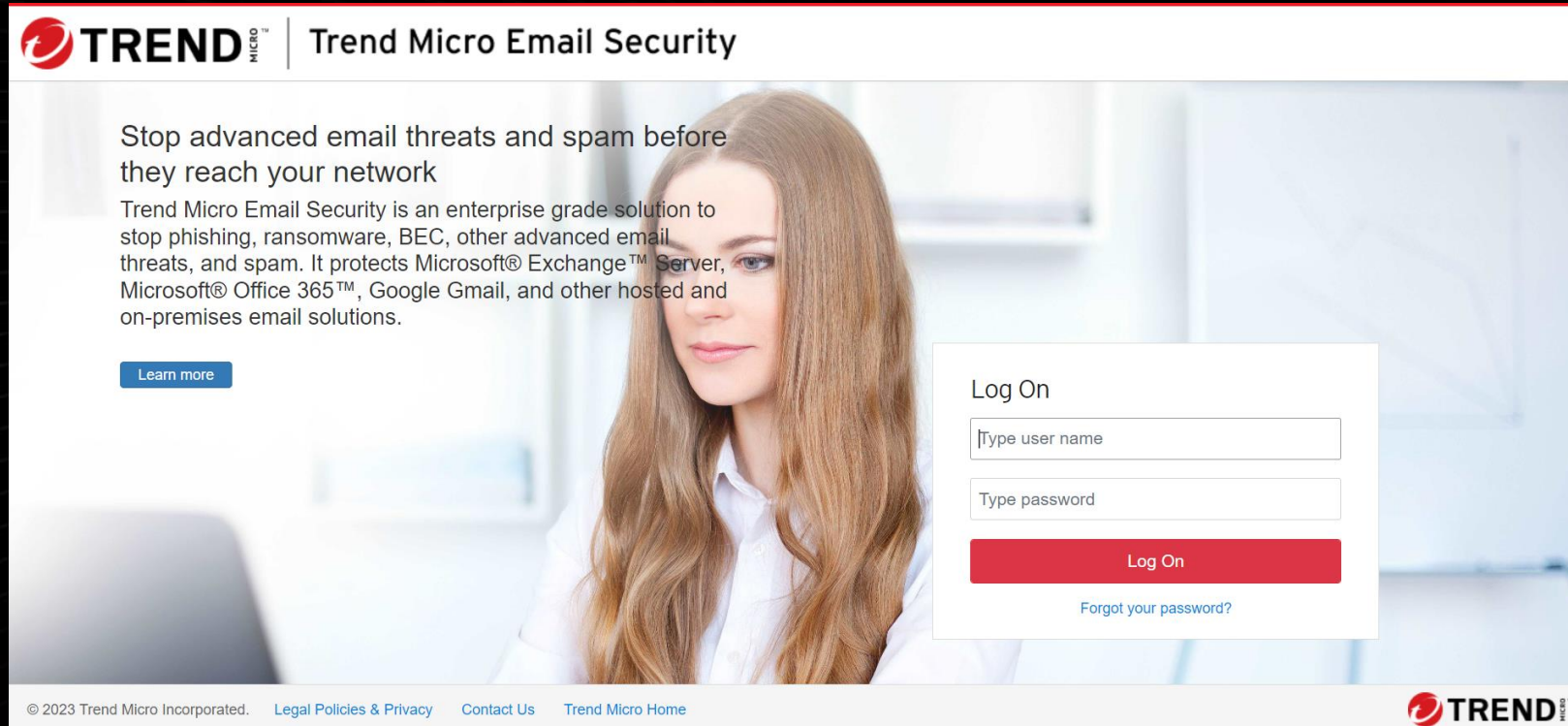
4

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



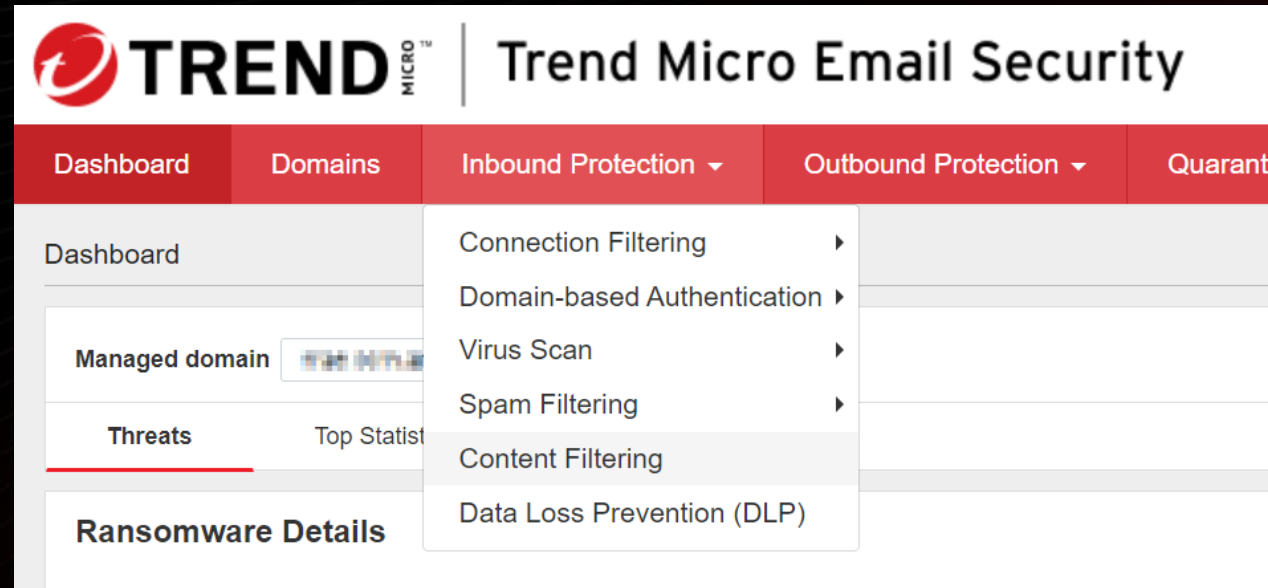
URL de Ingreso:

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

TMES

Tipos de Políticas

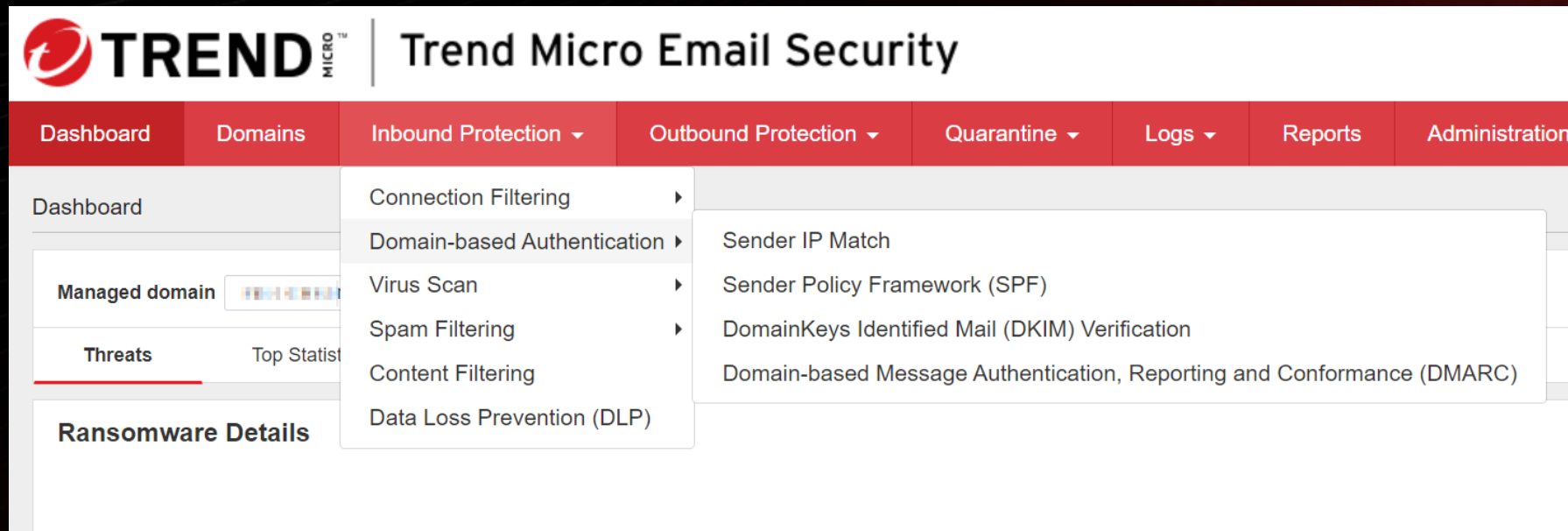
- Políticas divididas en “Protección Entrante o Protección Saliente” y subdivididas en distintas features de seguridad



Controles de Autenticación de dominios

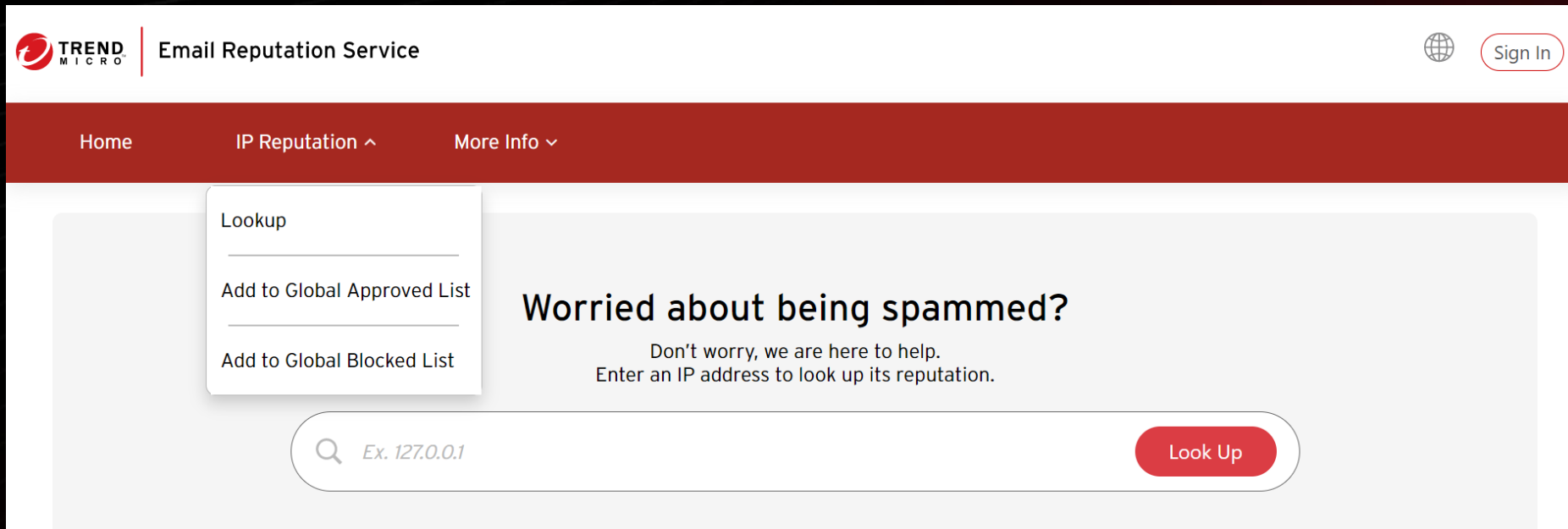
Existen tres tipos de chequeos aplicables sobre ambas plataformas:

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



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).



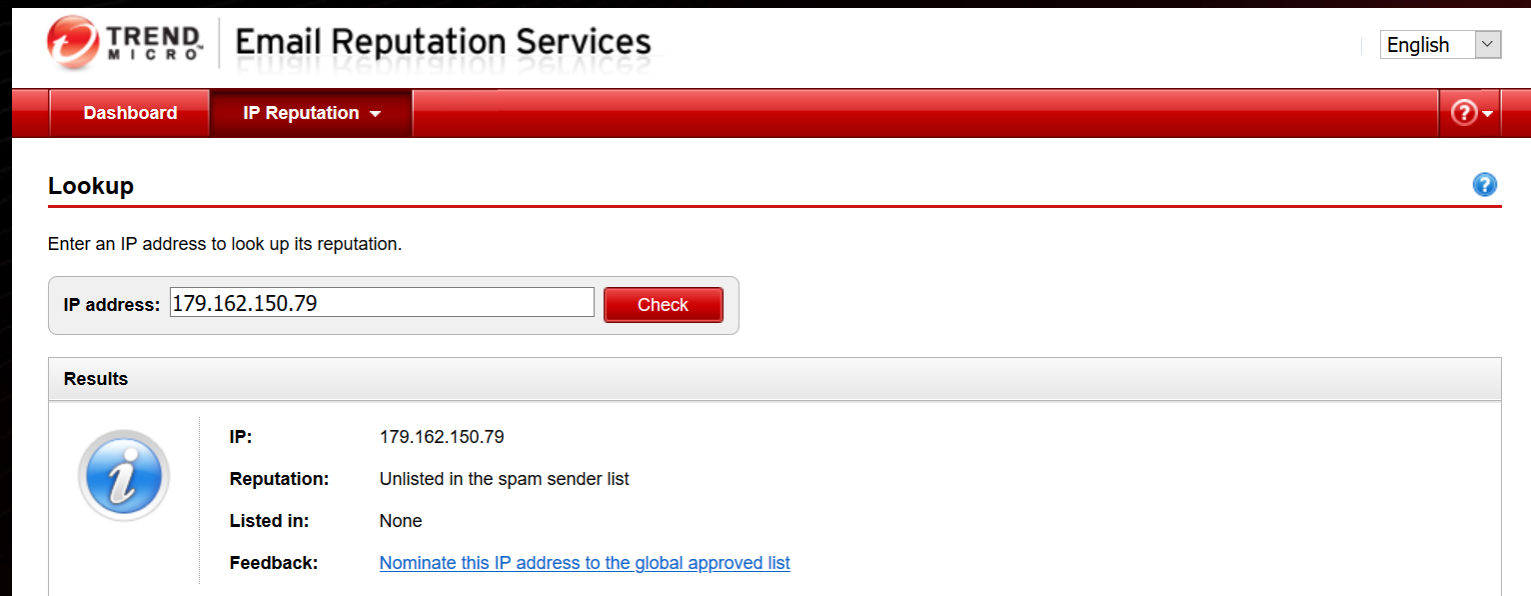
The screenshot shows the Trend Micro Email Reputation Service web interface. At the top, there is a header with the Trend Micro logo and the text "Email Reputation Service". To the right of the header is a "Sign In" button. Below the header is a navigation bar with links for "Home", "IP Reputation ^",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

<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' title are visible, along with a language dropdown set to 'English'. A navigation bar includes 'Dashboard' and 'IP Reputation'. The 'Lookup' section prompts the user to 'Enter an IP address to look up its reputation.' Below this, an input field contains '179.162.150.79' and a red 'Check' button. The 'Results' section shows the following data:

Results	
	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

 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:
Press ENTER to separate entries.

Sender:
Press ENTER to separate entries.

Subject:

Visibility:
All

Reason:
All

Rule:

Search

Delete

Deliver

Set Download Password

Records: 0 - 0 / 0 | 10 per page

Date	Sender	Recipient	Subject	Reason	Rule
No data to display.					

Delete

Deliver

Records: 0 - 0 / 0 | 10 per page

TMES

Configuración de la EUQ

The screenshot displays the Trend Micro Email Security (TMES) Administration console. The breadcrumb trail indicates the path: Administration > End User Management > Logon Methods. The interface is divided into two main sections: Local Account Logon and Single Sign-On.

Local Account Logon

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.

- Local account logon: ☒ Enabled
- Enforce two-factor authentication: ☐ Disabled
- Source of managed accounts: Aliaes synchronized from directories (dropdown menu)

Single Sign-On

This method allows end users to log on to the End User Console with their existing corporate credentials through single sign-on (SSO).

Single sign-on: ☐ Disabled

Below the Single Sign-On section, there is a table with columns: Profile, End User Console URL, Identity Provider, and Applied To. The table is currently empty, displaying "No data to display."

On the left side of the console, there is a sidebar with the following options:

- Sender Address Type
- Specify the type of sender address:
- ☒ Envelope address
- ☐ Message header
- ☐ Both
- Save button
- Cancel button

Reporting - Email Security

 Trend Micro Email Security

UTC-03:00

DashboardDomainsInbound Protection ▼Outbound Protection ▼Quarantine ▼Logs ▼ReportsAdministration ▼Help ▼

Reports > My Reports

My ReportsSchedules

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 displays the Trend Micro Email Security web interface. The top navigation bar includes links for Dashboard, Domains, Inbound Protection, Outbound Protection, Quarantine, Logs, and Reports. The 'Logs' menu is expanded, showing options for Mail Tracking, Policy Events, and URL Click Tracking. The breadcrumb trail indicates the current location is 'Logs > Mail Tracking'.

A modal dialog box titled 'Add Syslog Server Profile' is open, overlaying the main interface. The dialog contains the following fields and controls:

- *Profile name:** A text input field.
- Description:** A large text area.
- *Server address:** A text input field.
- *Port:** A text input field.
- Protocol:** A dropdown menu with 'TCP' selected.
- Format:** A dropdown menu with 'Key value' selected.
- Severity:** A dropdown menu with 'Informational' selected.
- Facility:** A dropdown menu with 'user' selected.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

In the background, the 'Syslog Settings' page is visible, showing tabs for 'Syslog Forwarding' and 'Syslog Server Profiles'. The 'Syslog Server Profiles' tab is active, displaying a table with columns for 'Profile Name' and 'Description'. There are 'Add' and 'Delete' buttons above the table.

Below the dialog box, a search bar is visible with a 'More options' link and a 'Search' button.

Integración con Vision One

The screenshot displays the Trend Vision One™ Product Connector interface. On the left is a vertical sidebar with various icons, including a red 'X' icon. The main area features a 'Connect' button at the top. Below it is a table with columns: Product, Connection status, Data center, Identifier ⓘ, and Description. The table is currently empty, with a message stating: 'No product has been connected yet. Click Connect to connect your first Trend Micro product.' A 'Connect Product' button is located at the bottom right of the table area. A 'Connection Settings' dialog box is open on the right, showing a dropdown menu for 'Product' with 'Trend Micro Email Security' selected. The dialog lists several products: 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* (highlighted), and Trend Micro Web Security. At the bottom of the dialog 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

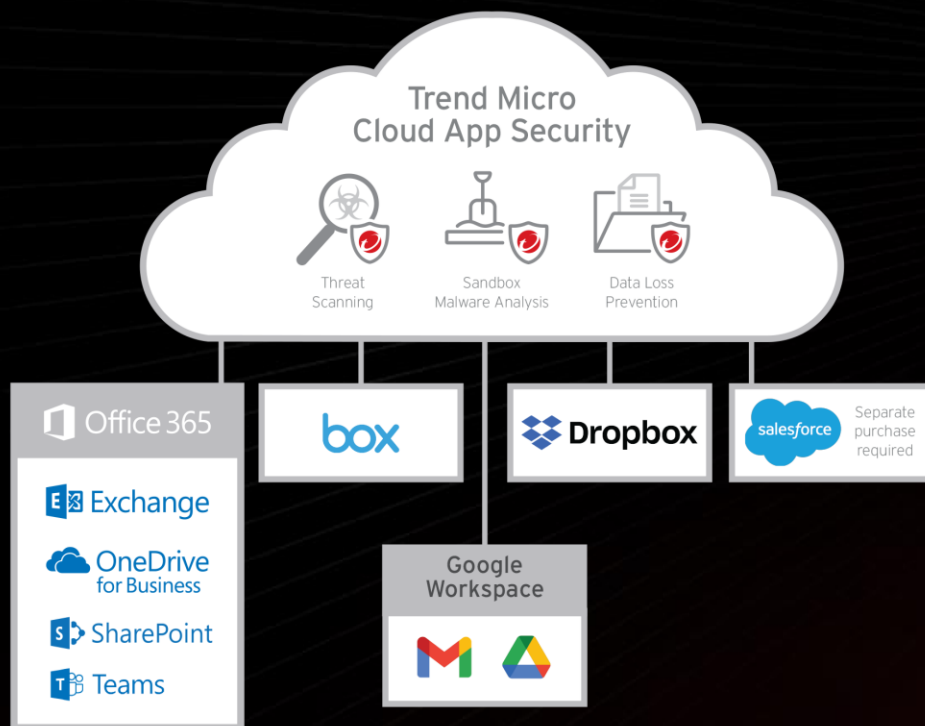


 **Microsoft**
Mail Gateway

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



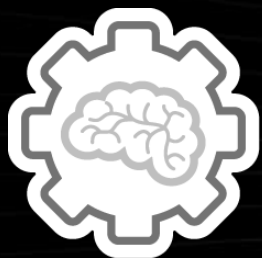
Análisis en
Sandbox



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	AS OS WD VA	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

- ☐

Note Manual scan does not include Virtual Analyzer scanning.

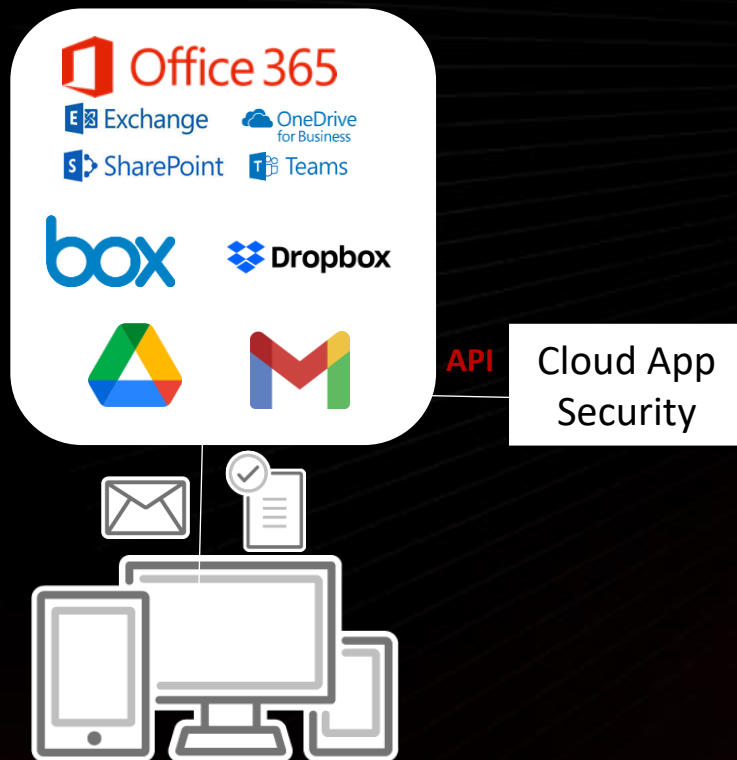
La importancia del escaneo manual que se realiza en tiempo real.

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



~~MX
Record~~

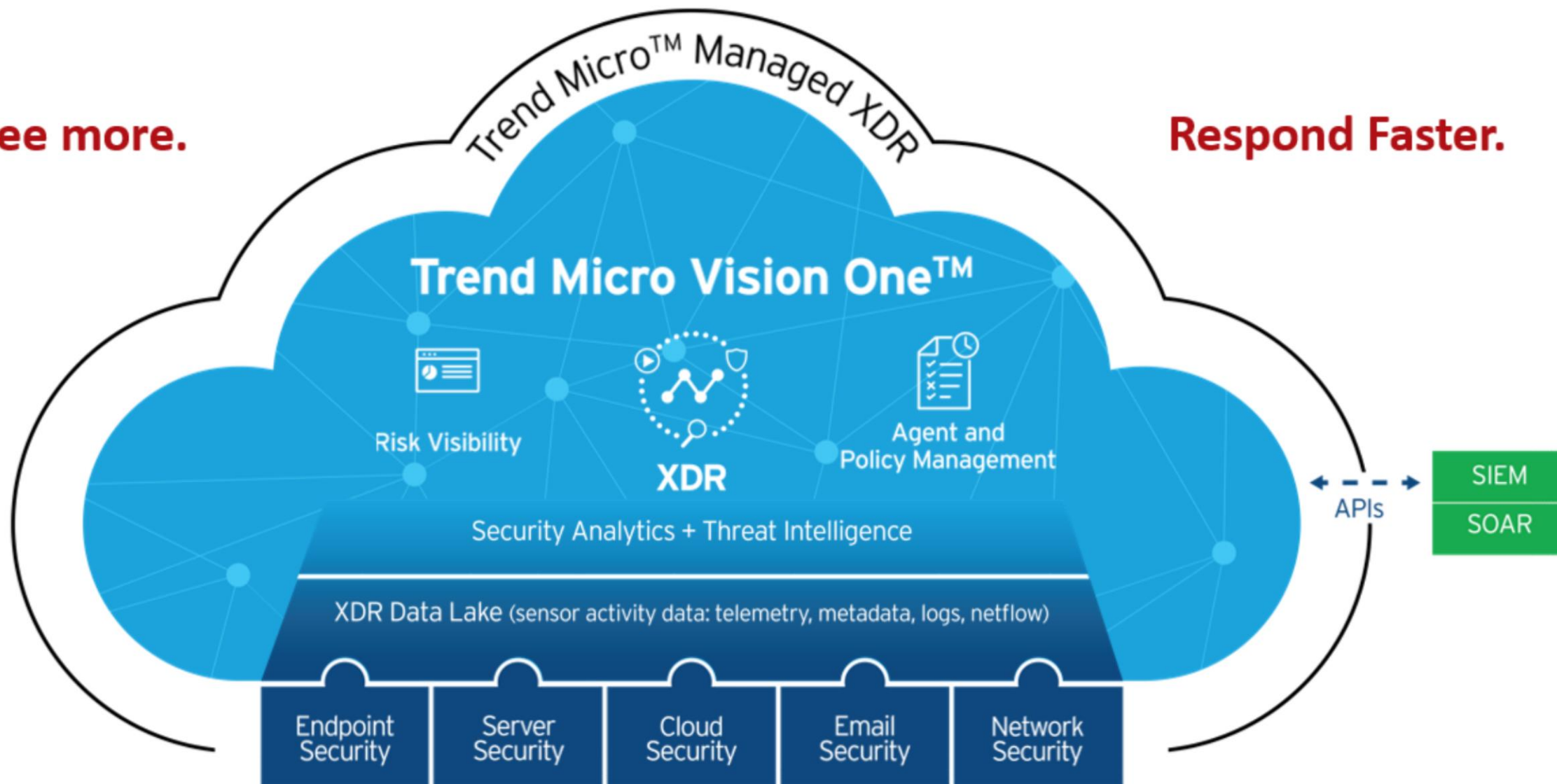
~~Software~~

~~User
settings~~

~~Web
proxy~~

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
☐	tmcasex_...onmicrosoft.com	Exchange Online	N/A	[Migration Available] [Change Password]
☐	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

Add ▾		Delete	Copy	Run Manual Scan	Internal Domains	← Previous 1 Next →		Search:
Priority ⓘ	Policy				Targets		Rules	
Exchange Online Policies Blocked Lists for Exchange Online enabled ⓘ								
☐ 1	☒ ON Exchange Policy				All Users		    	
☐ 2	☐ OFF Default Exchange Policy ATP DEFAULT POLICY: Policy used if no other policy created for target				All Users		    	
OneDrive for Business Policies								
☐ 1	☒ ON OneDrive Policy DEFAULT POLICY: Policy used if no other policy created for target				All Users		   	
SharePoint Online Policies								
☐ 1	☒ ON 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 →								

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

 Cloud App Security

7 (7) 2 (2) Welcome demo ?

DashboardAdvanced Threat ProtectionData Loss PreventionLogsQuarantine

Service

Exchange Online

Security Filter

Advanced Threat Protection

Web Reputation

Malware Scanning

Affected User

instantdemo@productcloud.me

Status

Quarantined

DeleteFailure

Exchange Online

OneDrive for Business

SharePoint Online

Dropbox

7961

3992

3267

15220

15087

133

Search

Select Date Range

Search

RestoreDownloadDelete

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 day(s)



38 | ©2023 Trend Micro Inc.

Logs & Reporting

 Cloud App Security

DashboardAdvanced Threat ProtectionData Loss Prevention**Logs**Quarantine

TemplatesReportsScheduled Report

Search

Save...Export...Preview Report

Select Date RangeSearch

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

DROPBOX_SCHEDULED_SYNC

EXCHANGE_SCHEDULED_SYNC

ONEDRIVE_SCHEDULED_SYNC

SHAREPOINT_SCHEDULED_SYNC

CONNECT_TO_XDR

UPDATE_POLICY

ADD_AUTOMATION_API_AUTHENTICATIO...

DISCONNECT_FROM_XDR

645

51

19

655

91

90

90

90

50

7

1

1



DEMOS

Actividad:

Reconocimiento de Phishing

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

¡Muchas Gracias!

