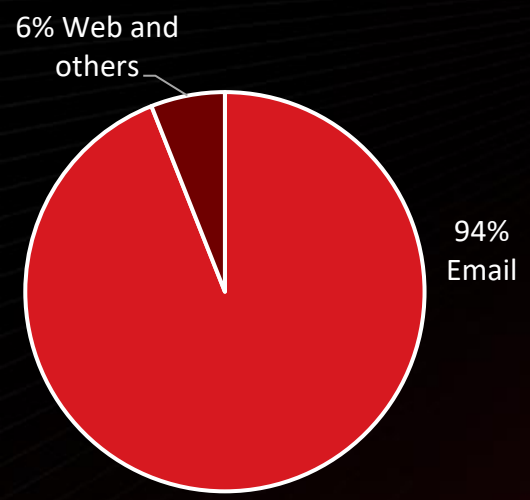
Email solutions
Trend Micro

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.

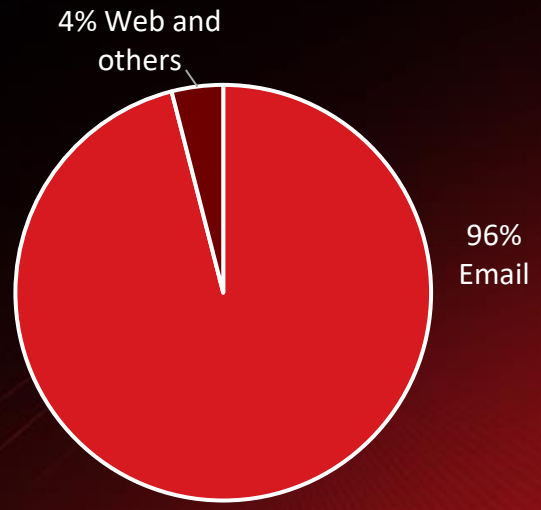
La mayoría de los ciberataques provienen del correo electrónico

Malware Delivery Method



Source: Verizon DBIR 2019

Social Engineering Attack Delivery Method



Source: Verizon DBIR 2020

Business Email Compromise (BEC) Attacks

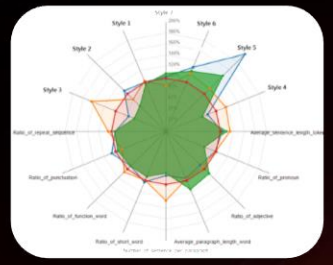
El impostor envía un correo electrónico a "Max" haciéndose pasar por "Eva"

Max,

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

Saludos,
Eva

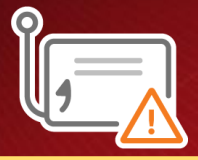
Office 365 Exchange



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
	...

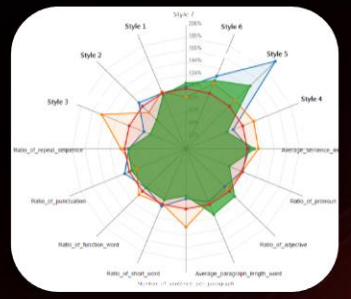
EXPERT RULES

MACHINE LEARNING

Mimics the decision making of a security expert

+

Authorship analysis



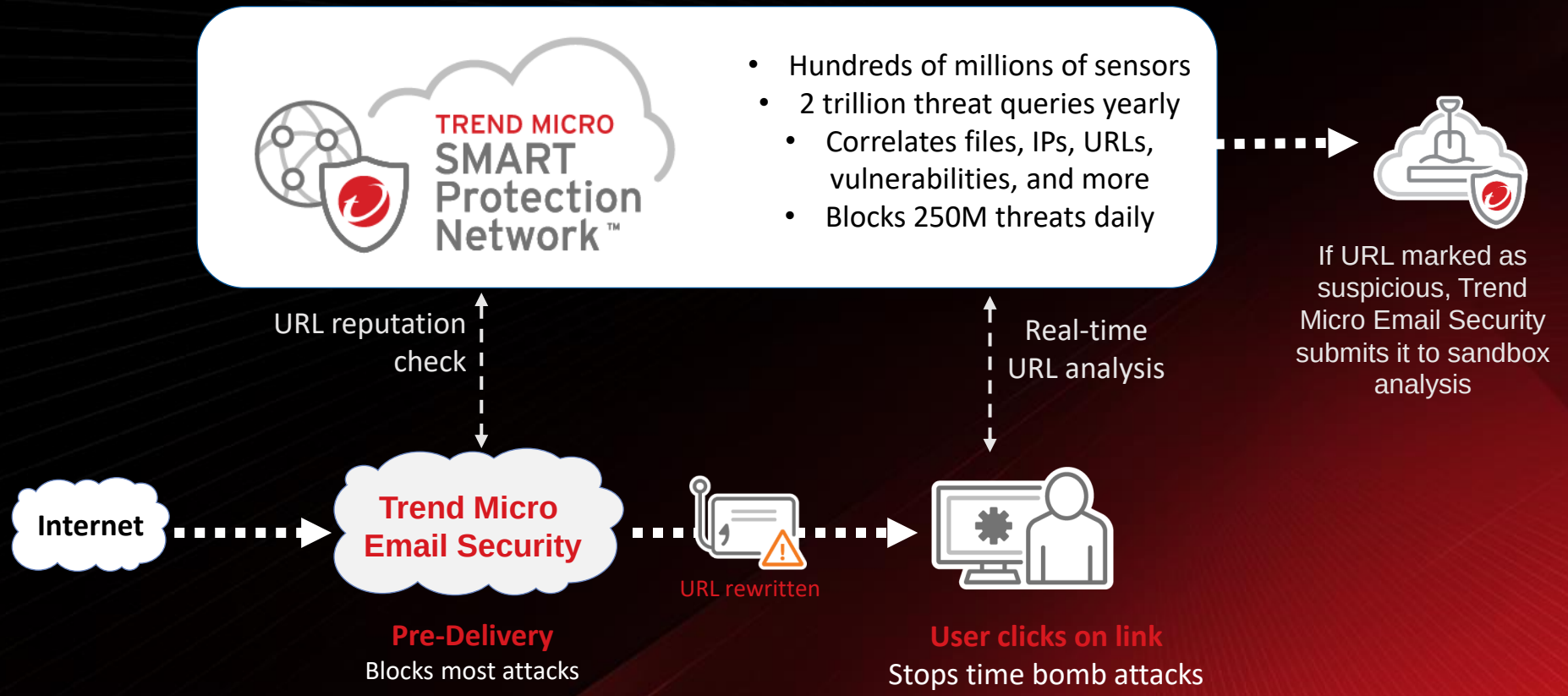
Compares a suspected impersonation to AI model of high-profile user's writing style

WRITING STYLE DNA

MACHINE LEARNING

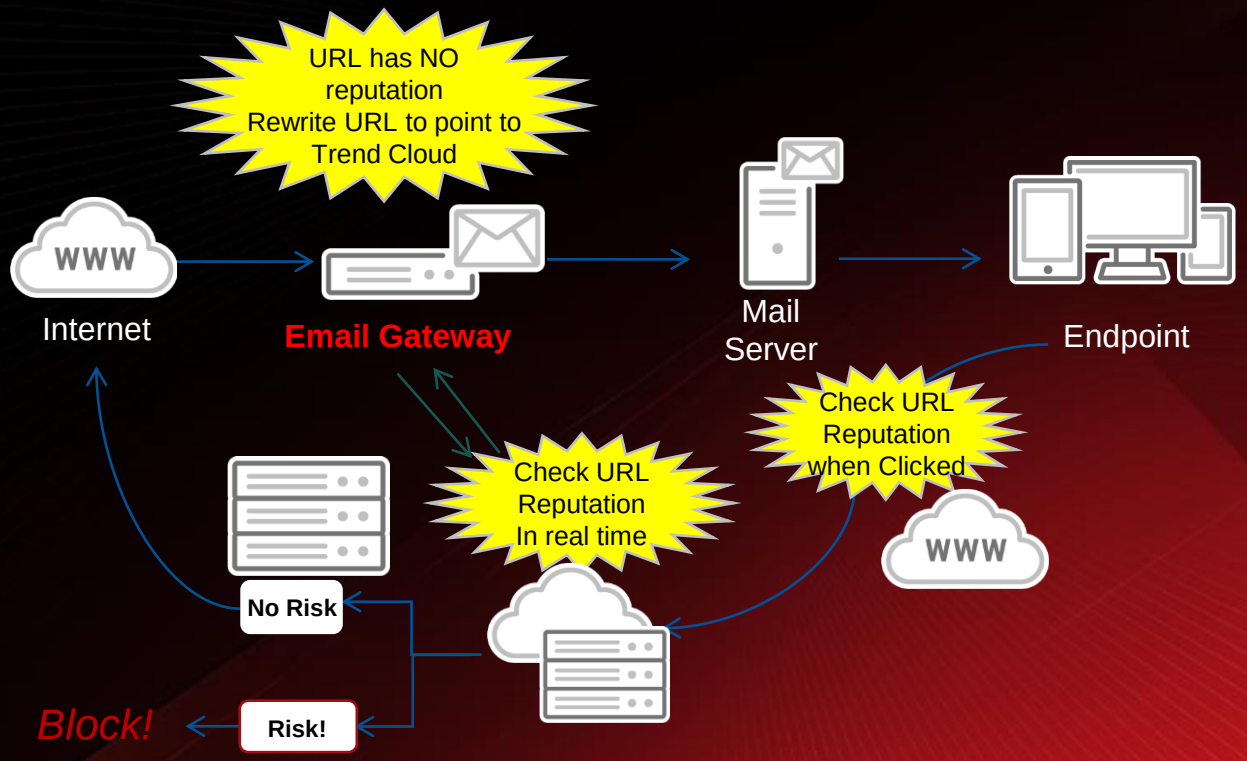
TREND MICRO

Malicious URL Protection

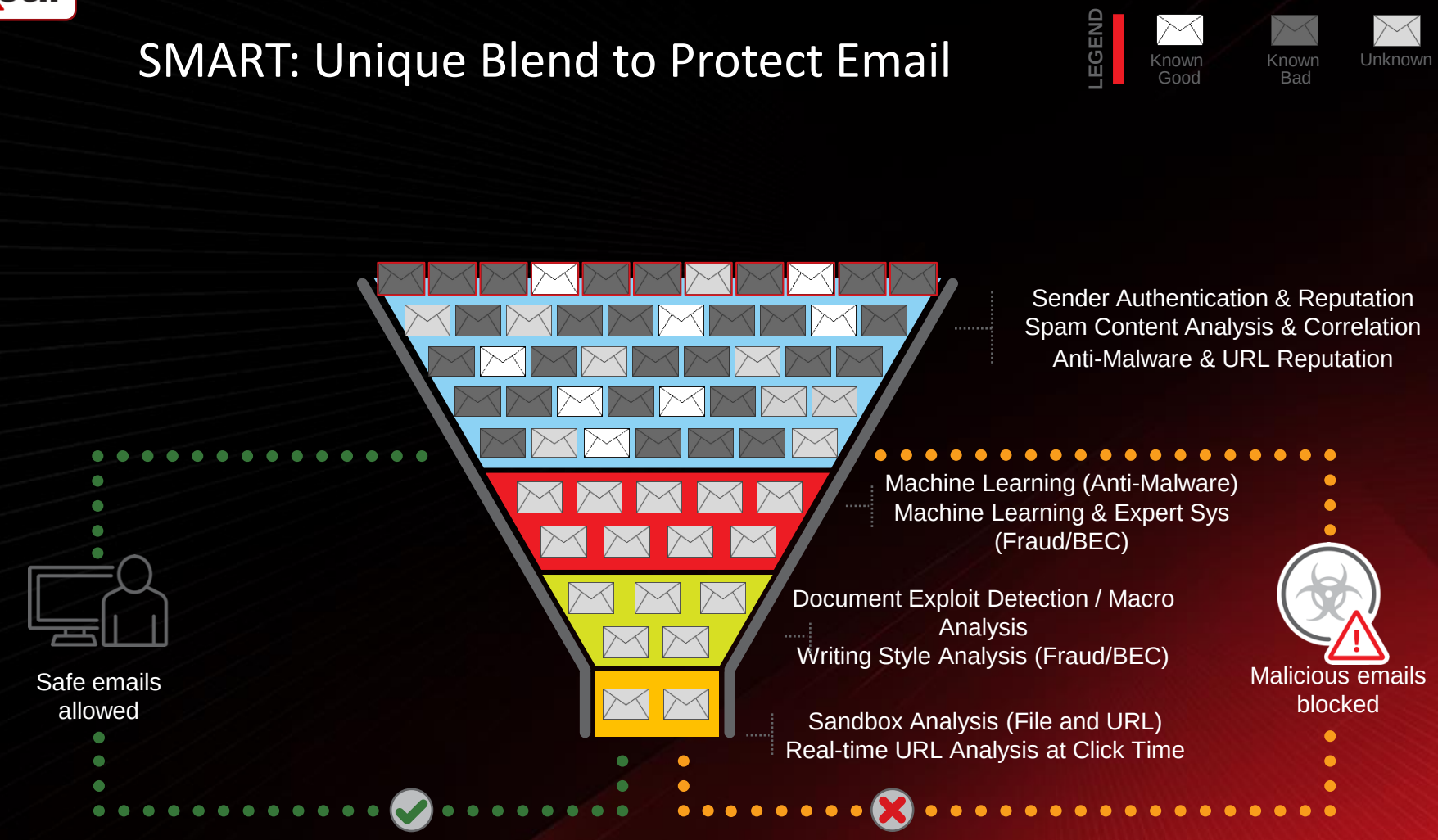


Threat detection – **URL Time Of Click**

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



SMART: Unique Blend to Protect Email

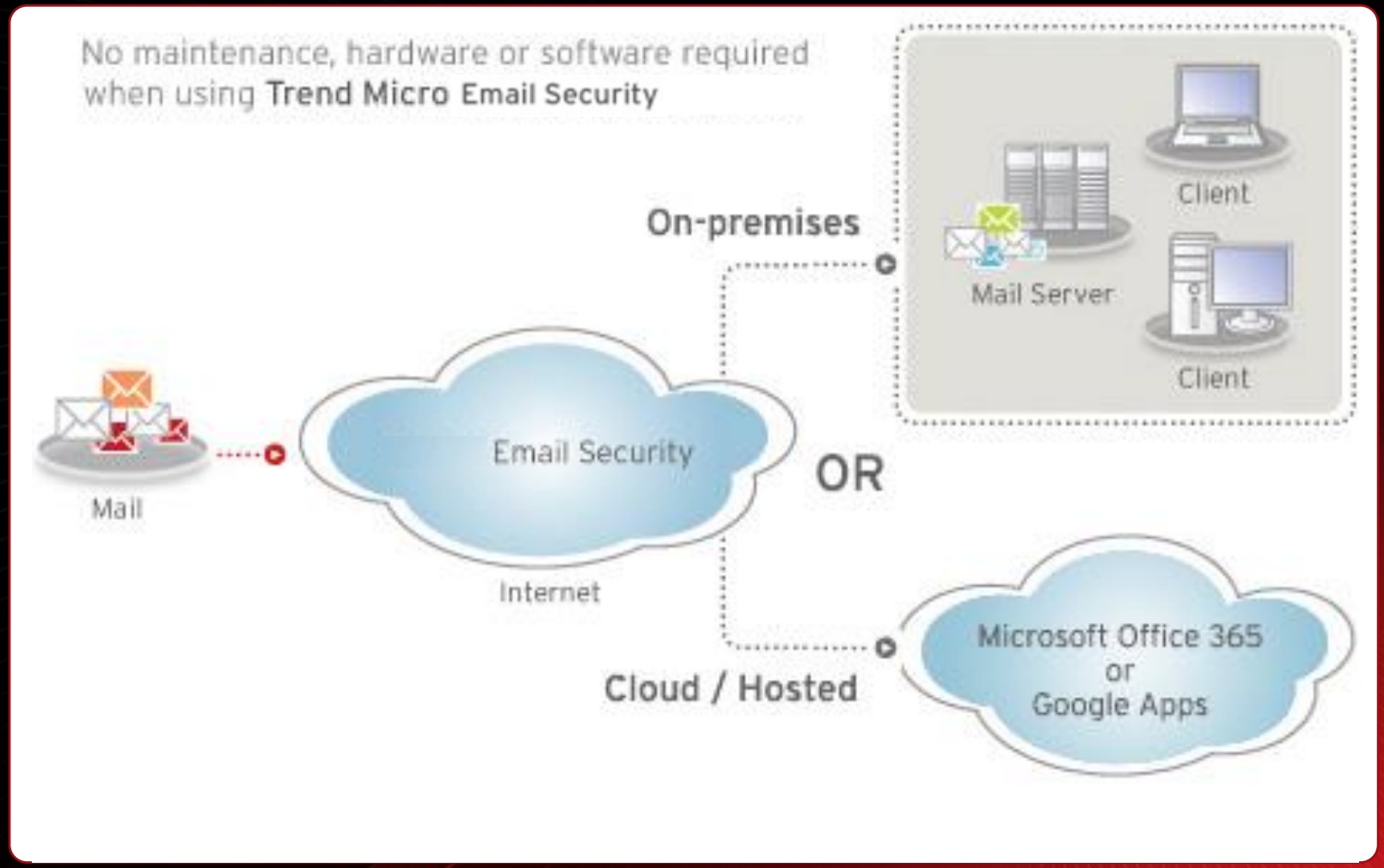


Trend Micro Email Security Portfolio

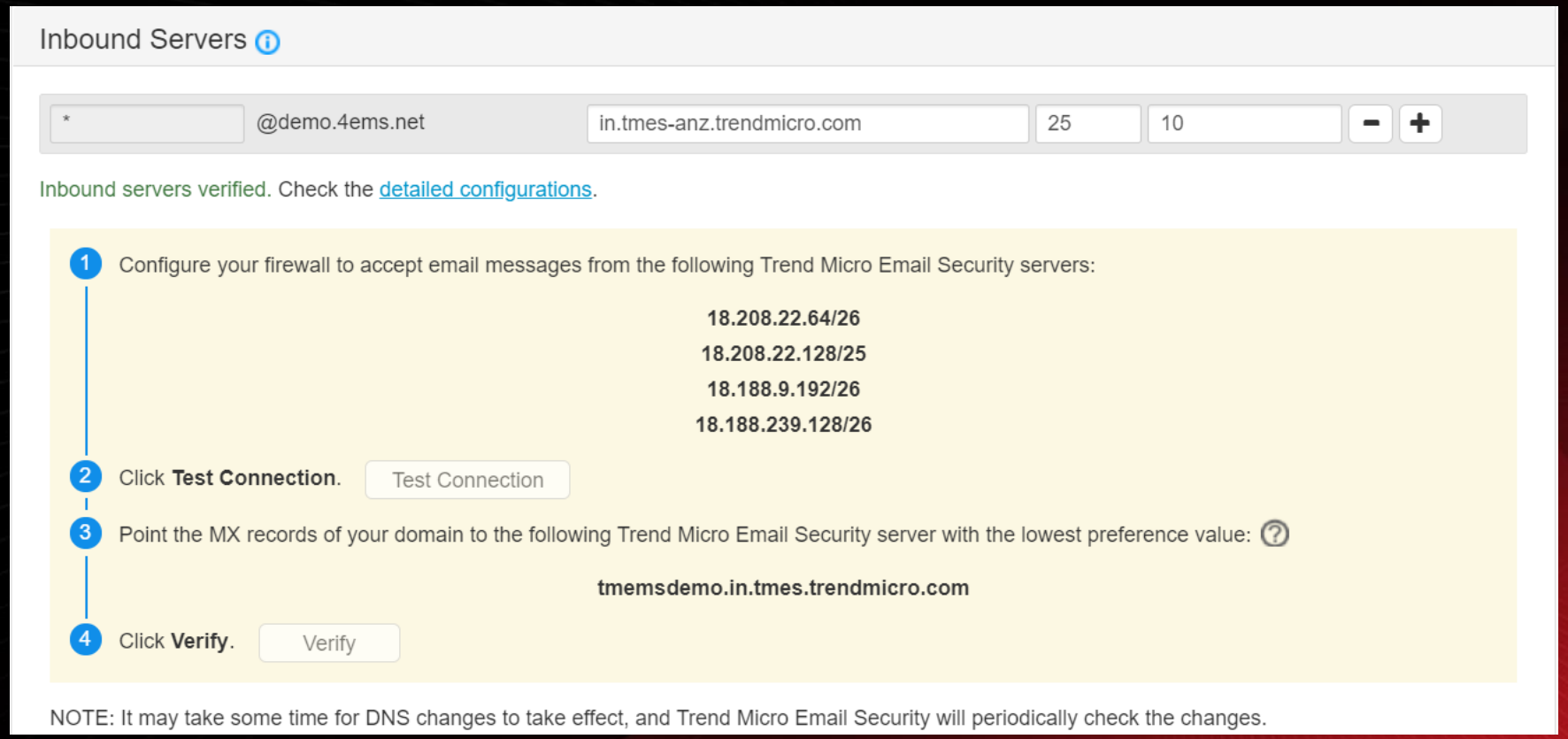
Trend Micro Email Solutions

Trend Micro Email Security (TMES)

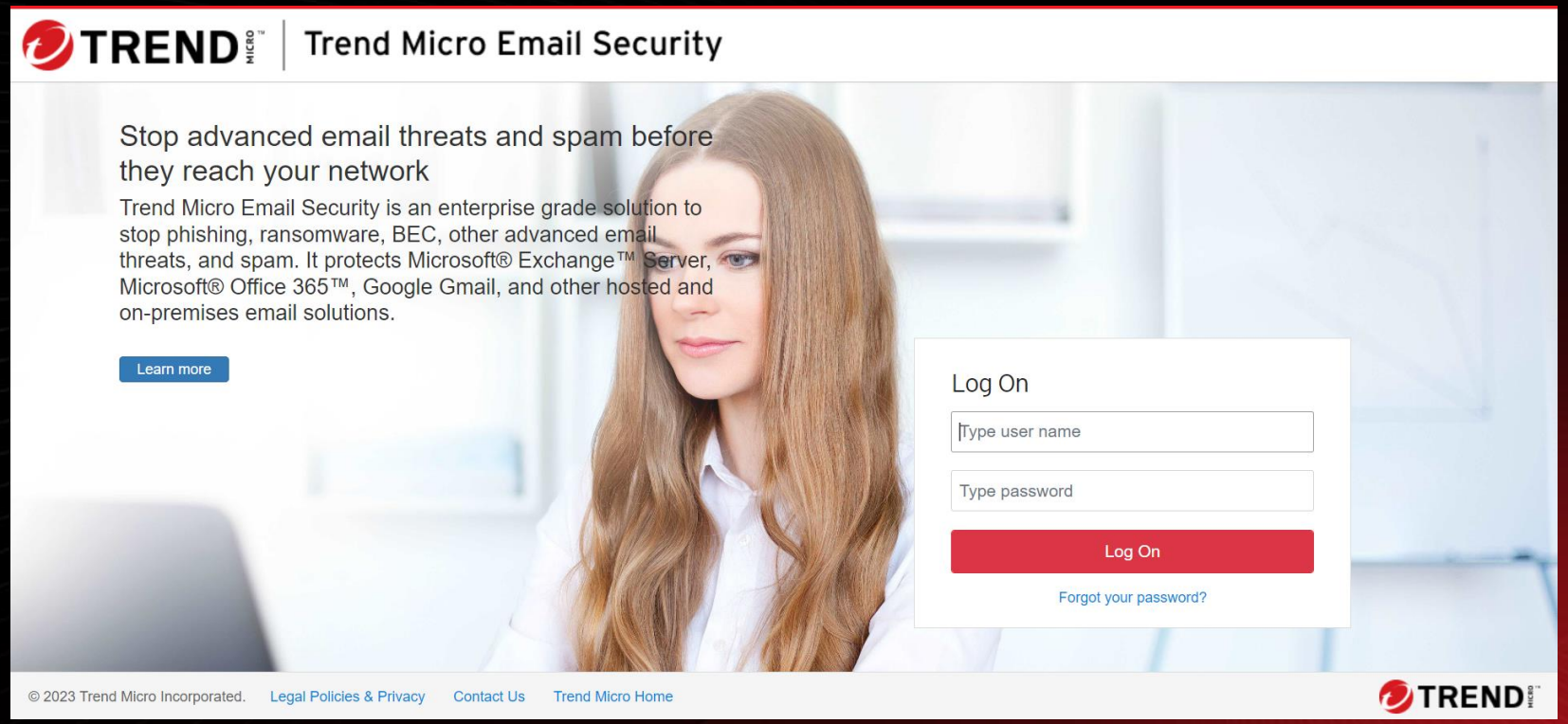
Deploy TMES (SaaS)



Deploy TMES (SaaS)



TMES
Consola Web de Administración



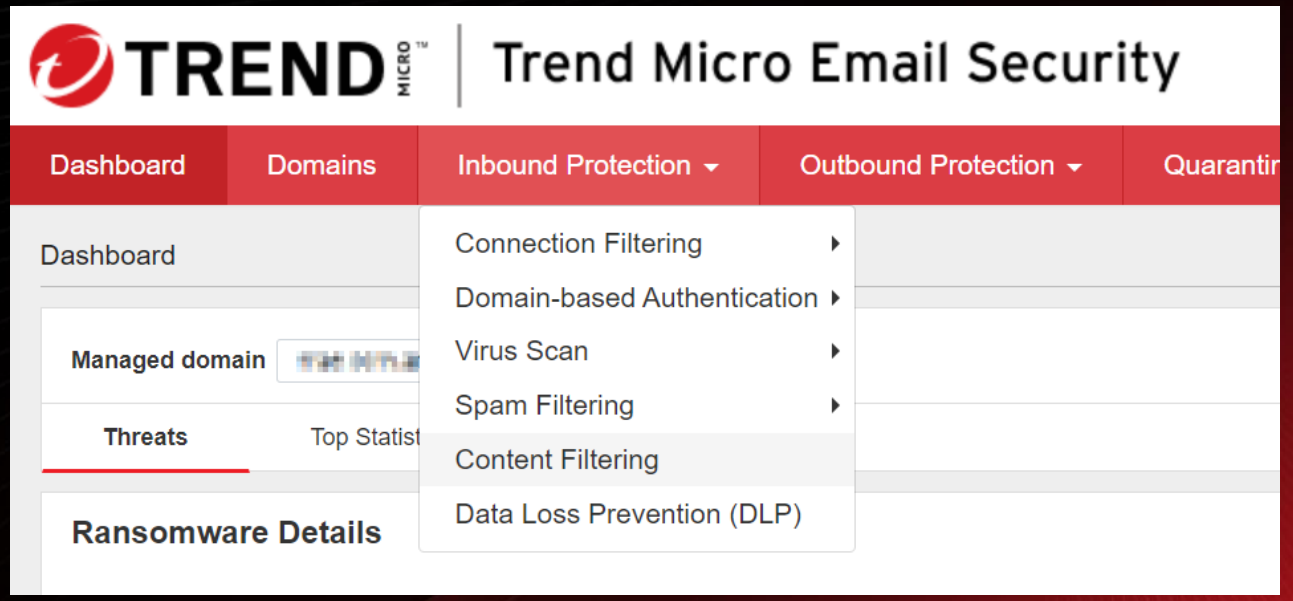
URL de Ingreso:

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

TREND MICRO

TMES
Tipos de Políticas

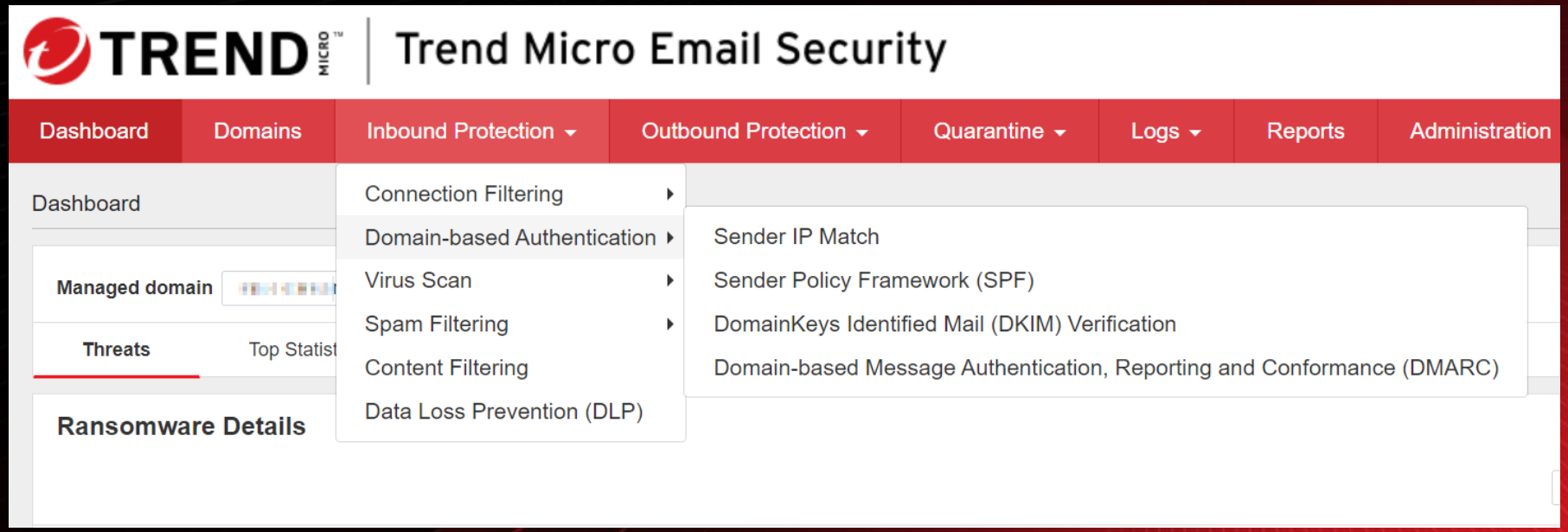
- Políticas divididas en “Protección Entrante o Protección Saliente” y subdivididas en distintas features de seguridad



Controles de Autenticación de dominios

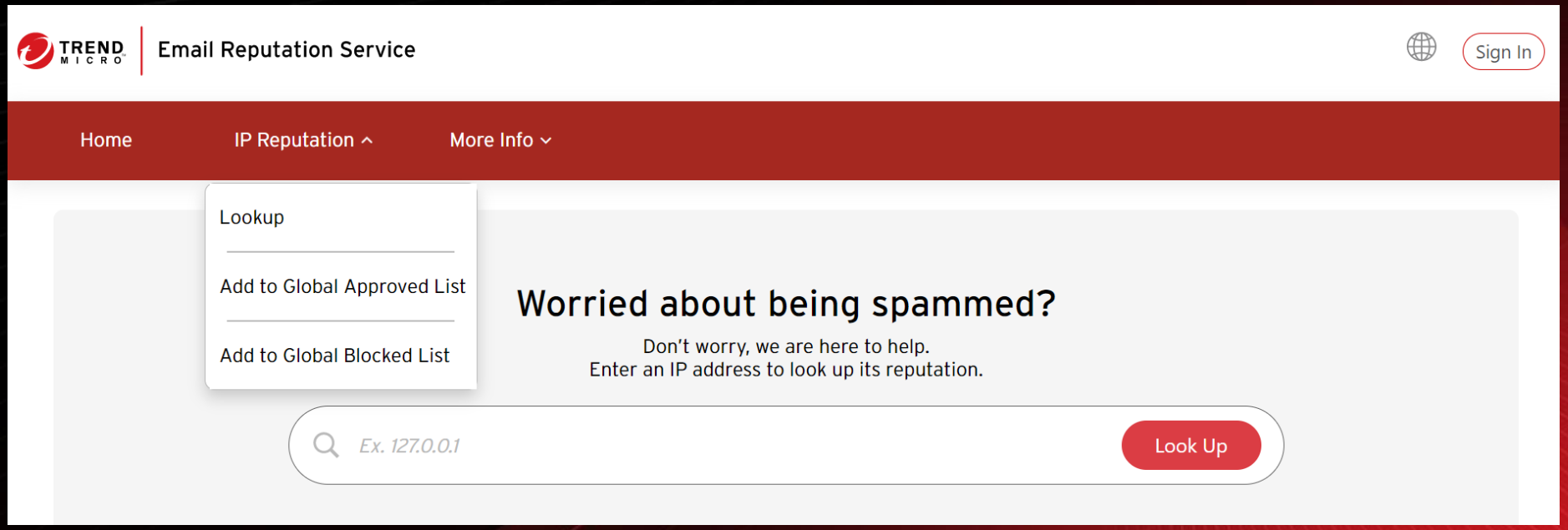
Existen tres tipos de chequeos aplicables sobre ambas plataformas:

- **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).

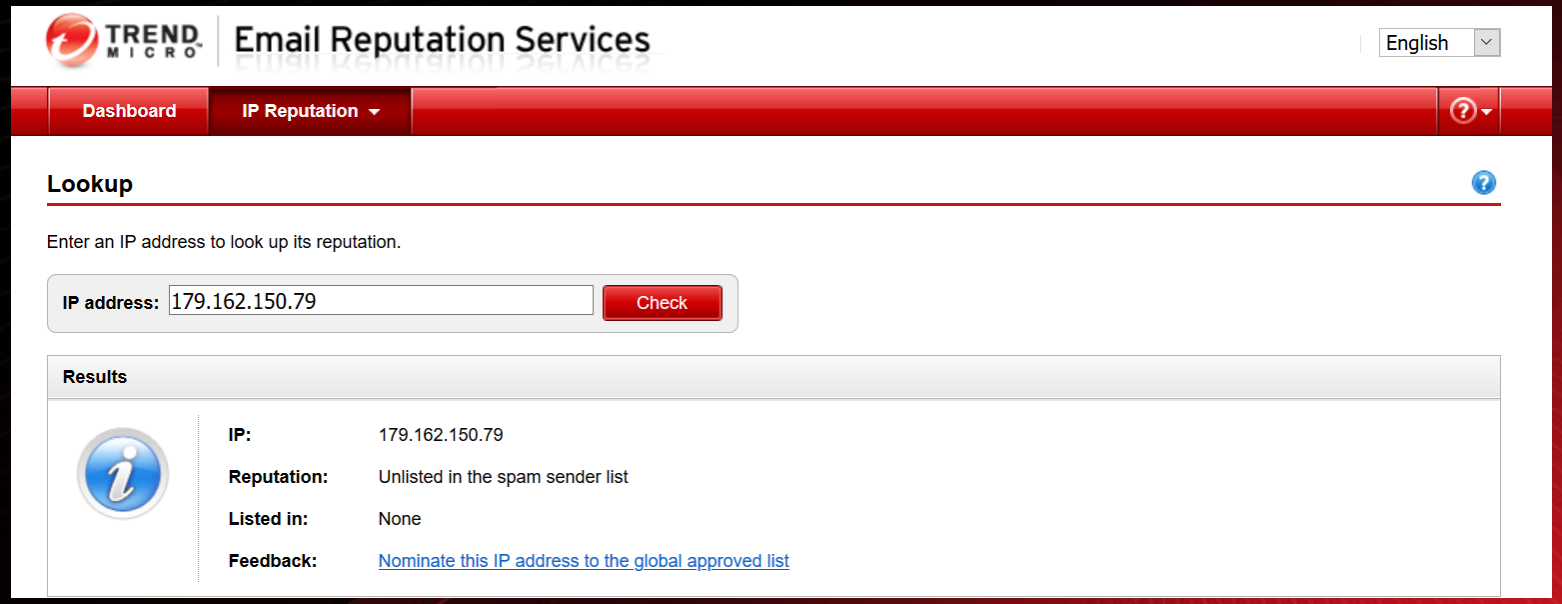


https://servicecentral.trendmicro.com/en-US/ers/

Email Reputation

Tipos de listas de reputación:

- RBL
- QIL
- DUL

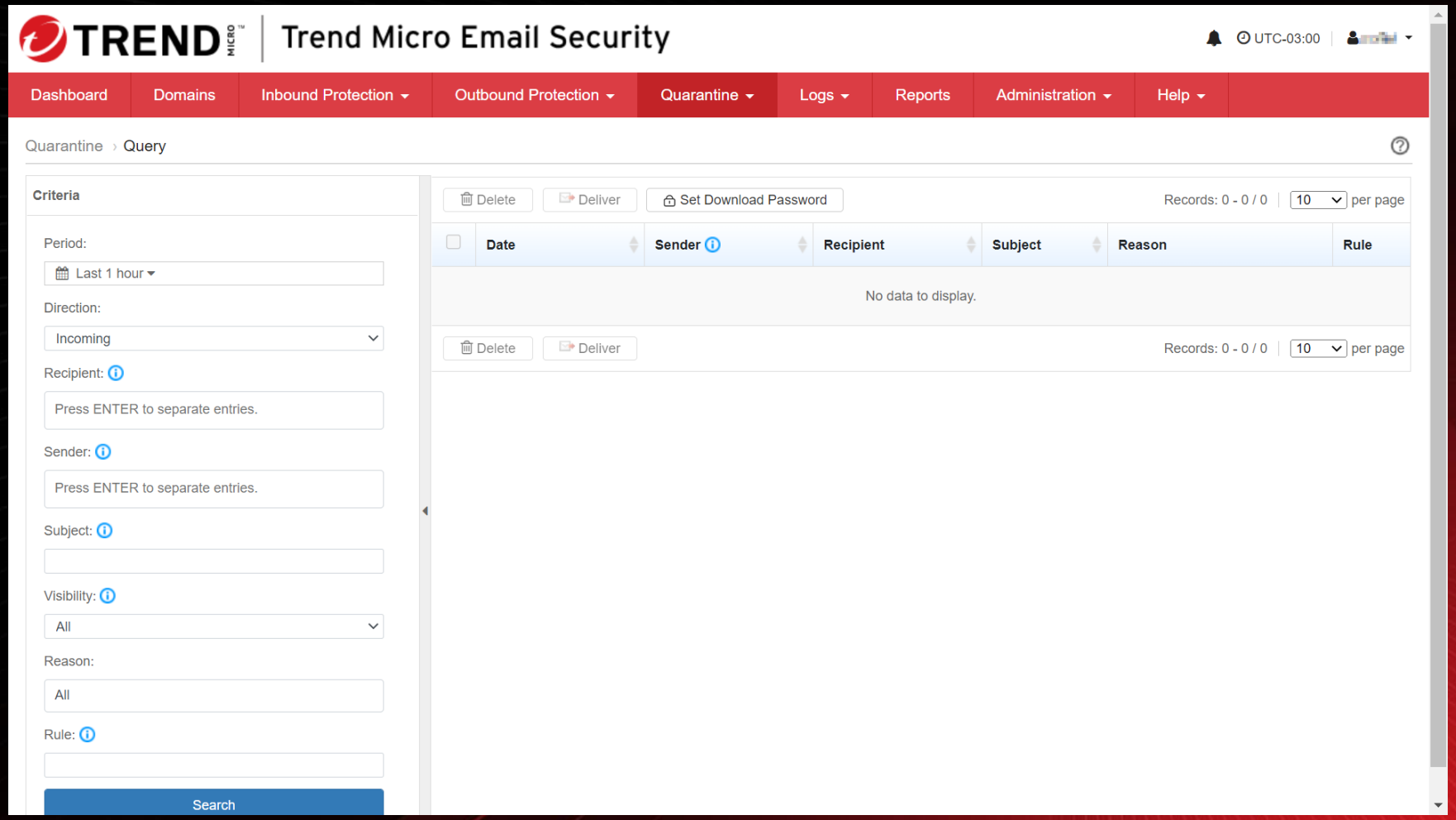


Areas de Almacenamiento

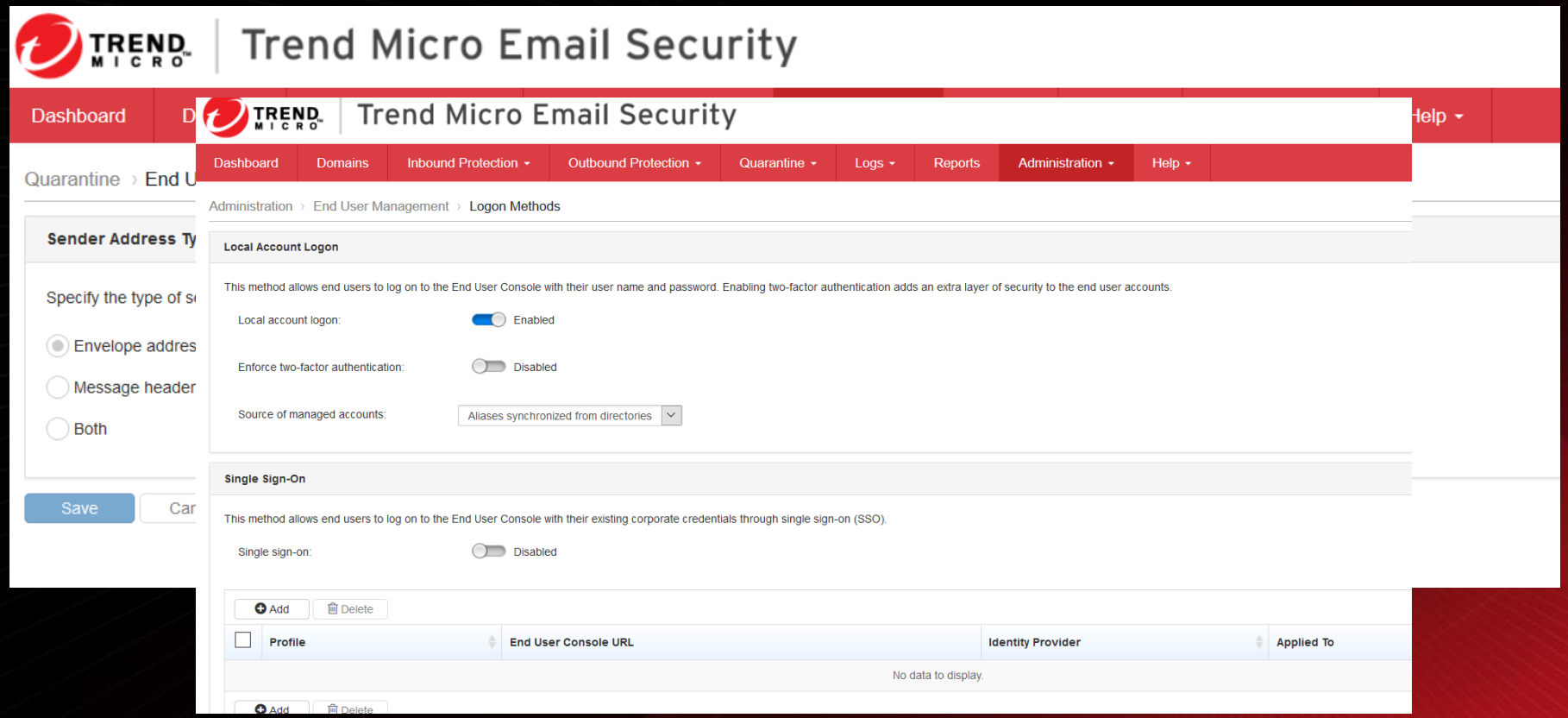
- **Quarantines** Almacena los correos “no deseados” definidos por política para ser enviados a cuarentena.

- **Deferred** Almacena los correos que no pueden ser enviados por algún motivo (problema de la propia Plataforma o del servidor que debe recibirlo).

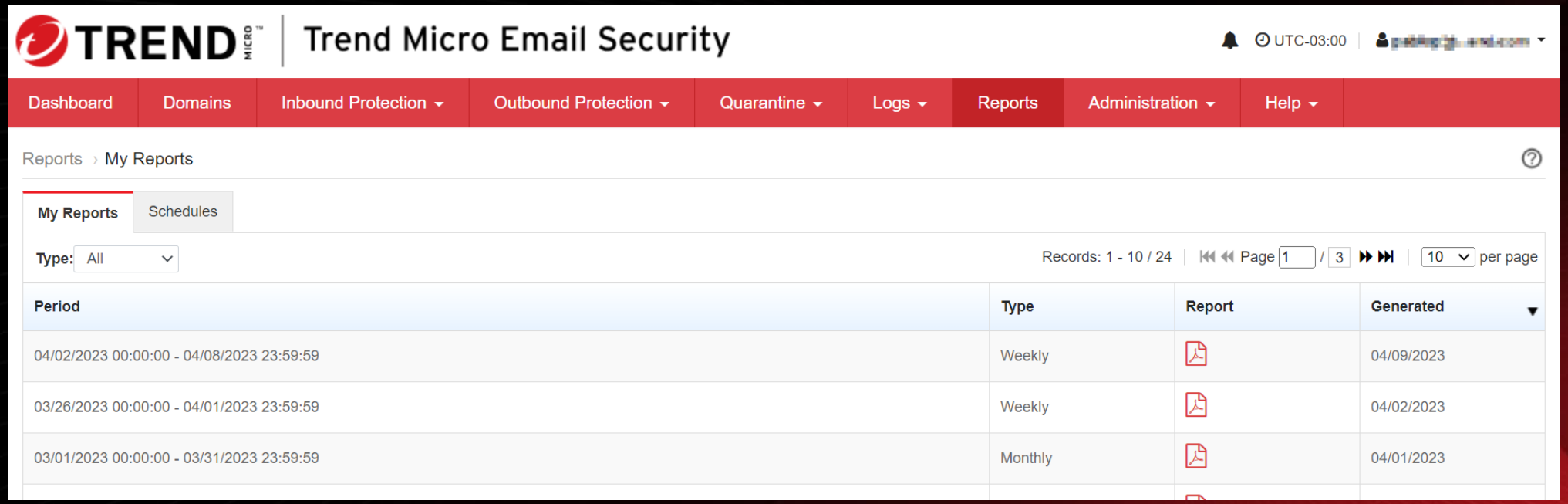
TMES
Administración de la cuarentena



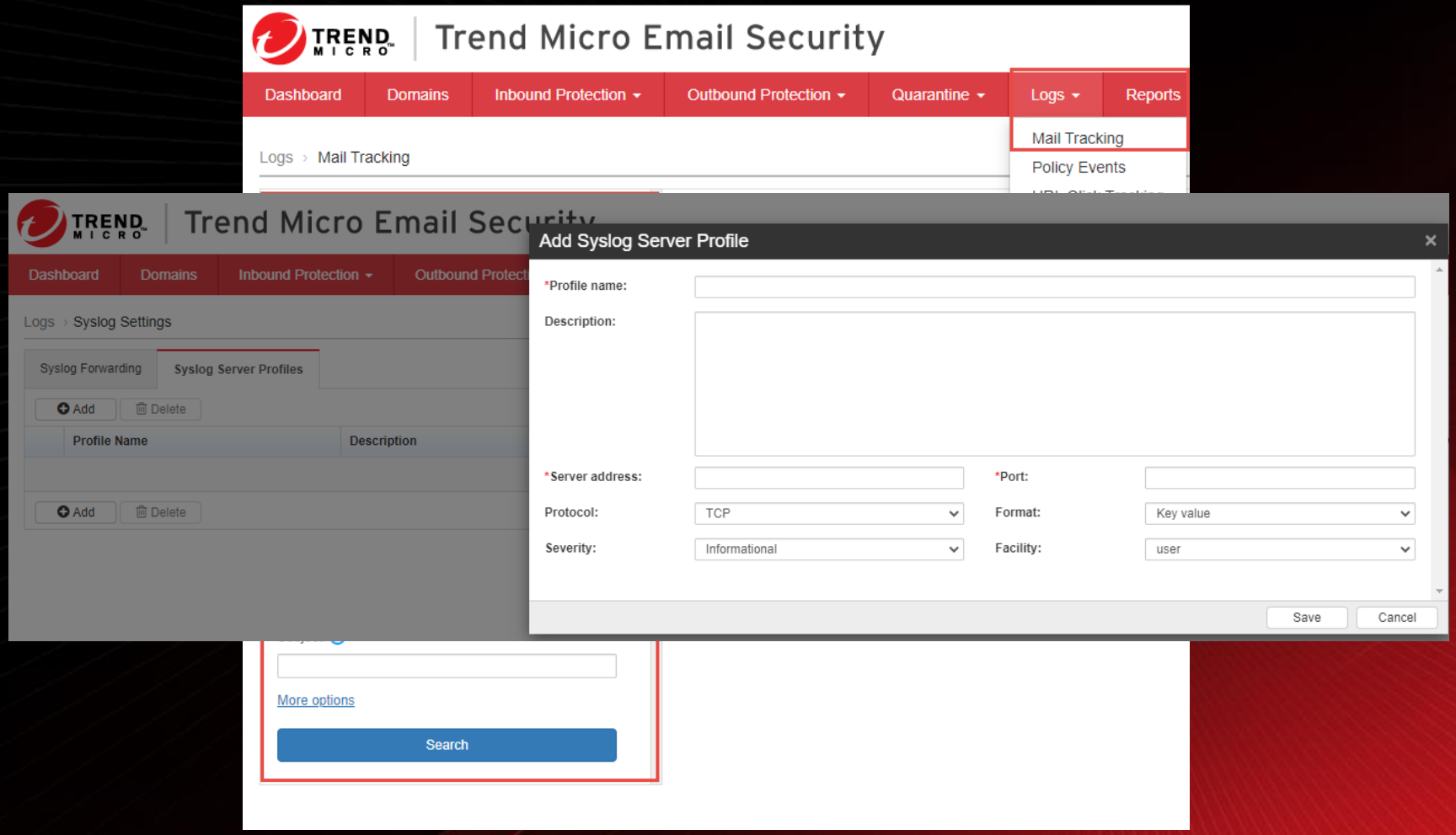
TMES
Configuración de la EUQ



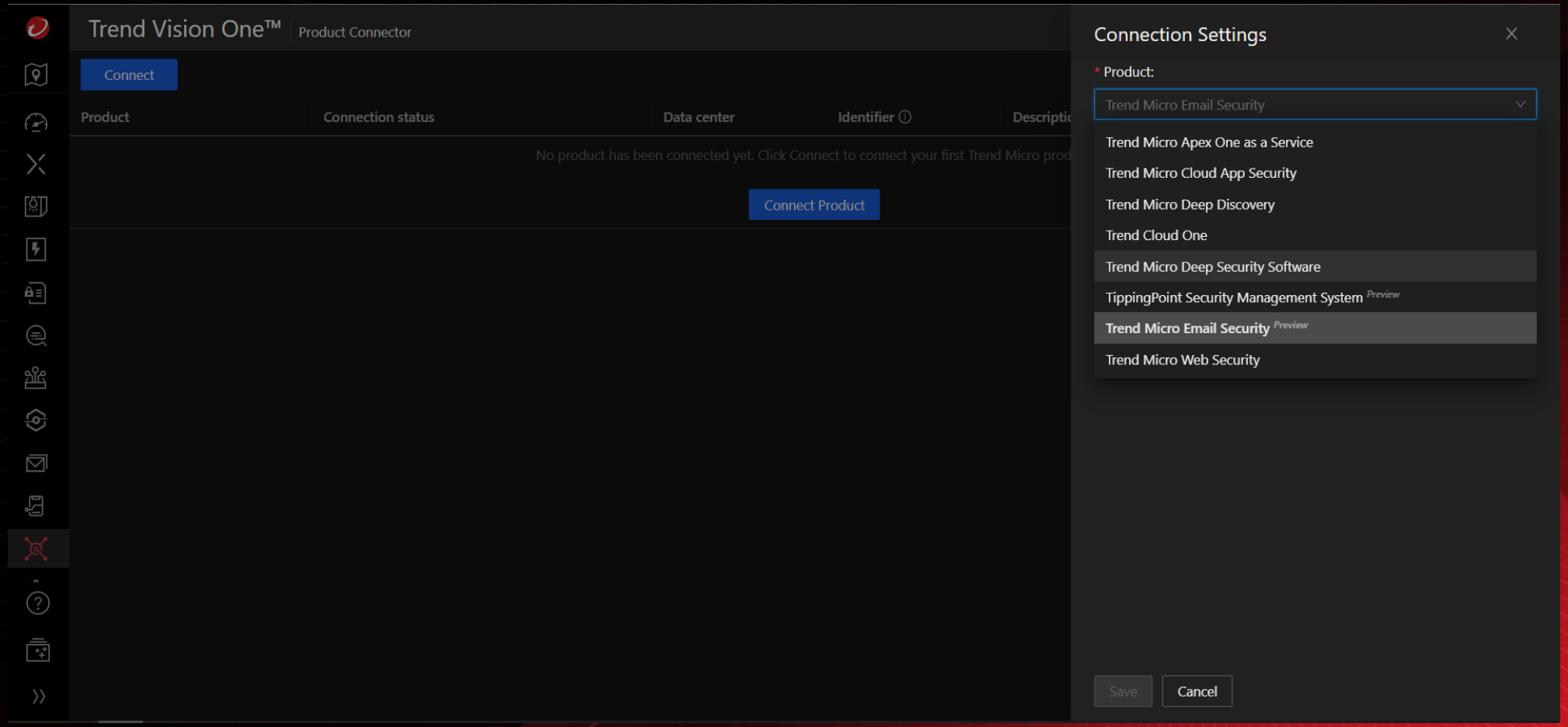
Reporting - Email Security



Logs – Email Security



Integración con Vision One



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

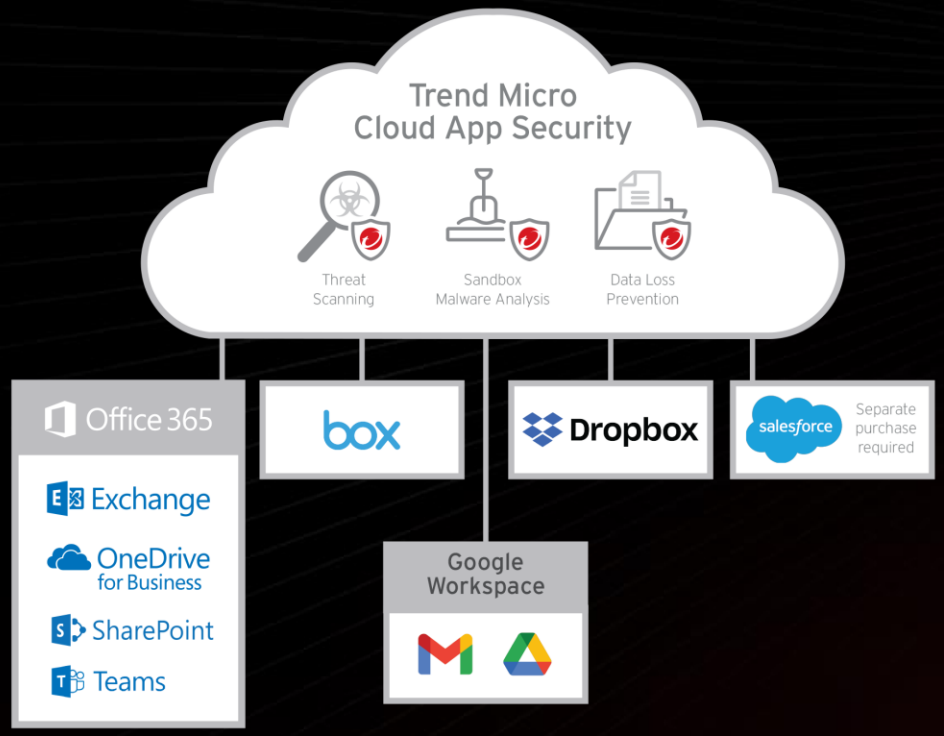
Email Gateway

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 amenzas conocidas

- Firmas de malware
- Reputación web y URL

Trend Micro Cloud App Security (CAS)

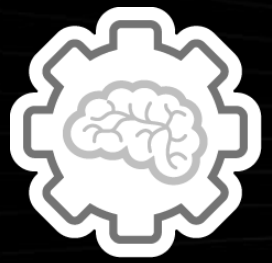
Bloquea amenzas conocidas

- 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 busqueda de exploits conocidos y posibles.

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

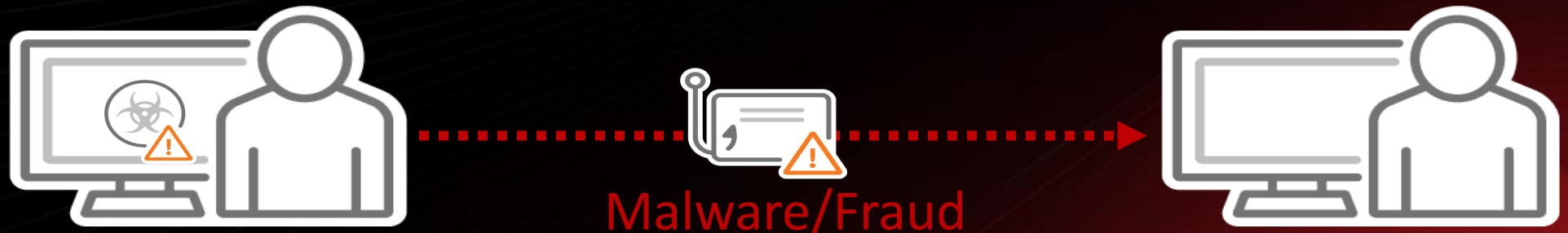
Detecte los ataques que ya están dentro de su organización

Disponible a través de la integración de servicios (CAS)

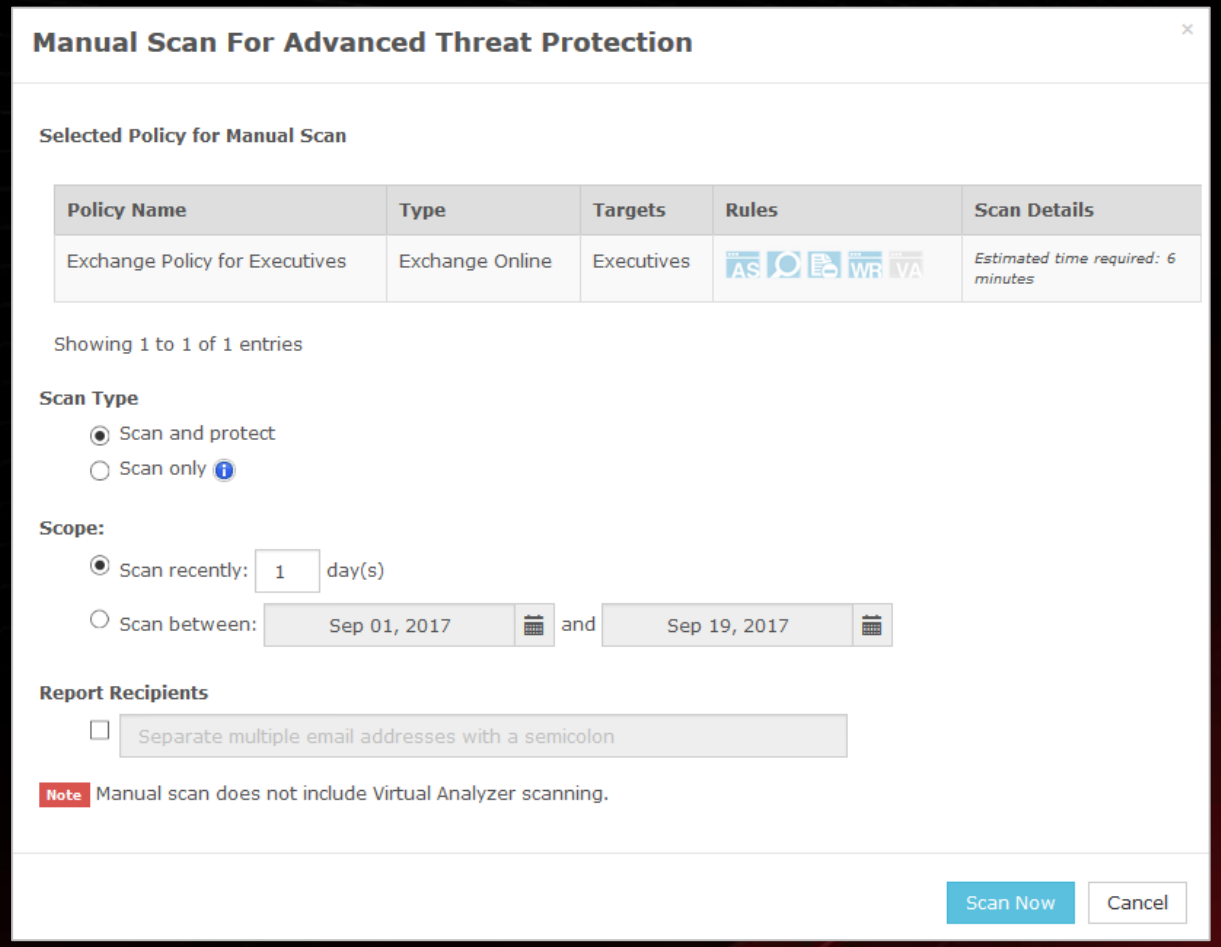
Inspecciona el correo electrónico interno en busca de amenazas avanzadas y fraude

Políticas granulares por grupo de AD

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



Respuesta y reparacion



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

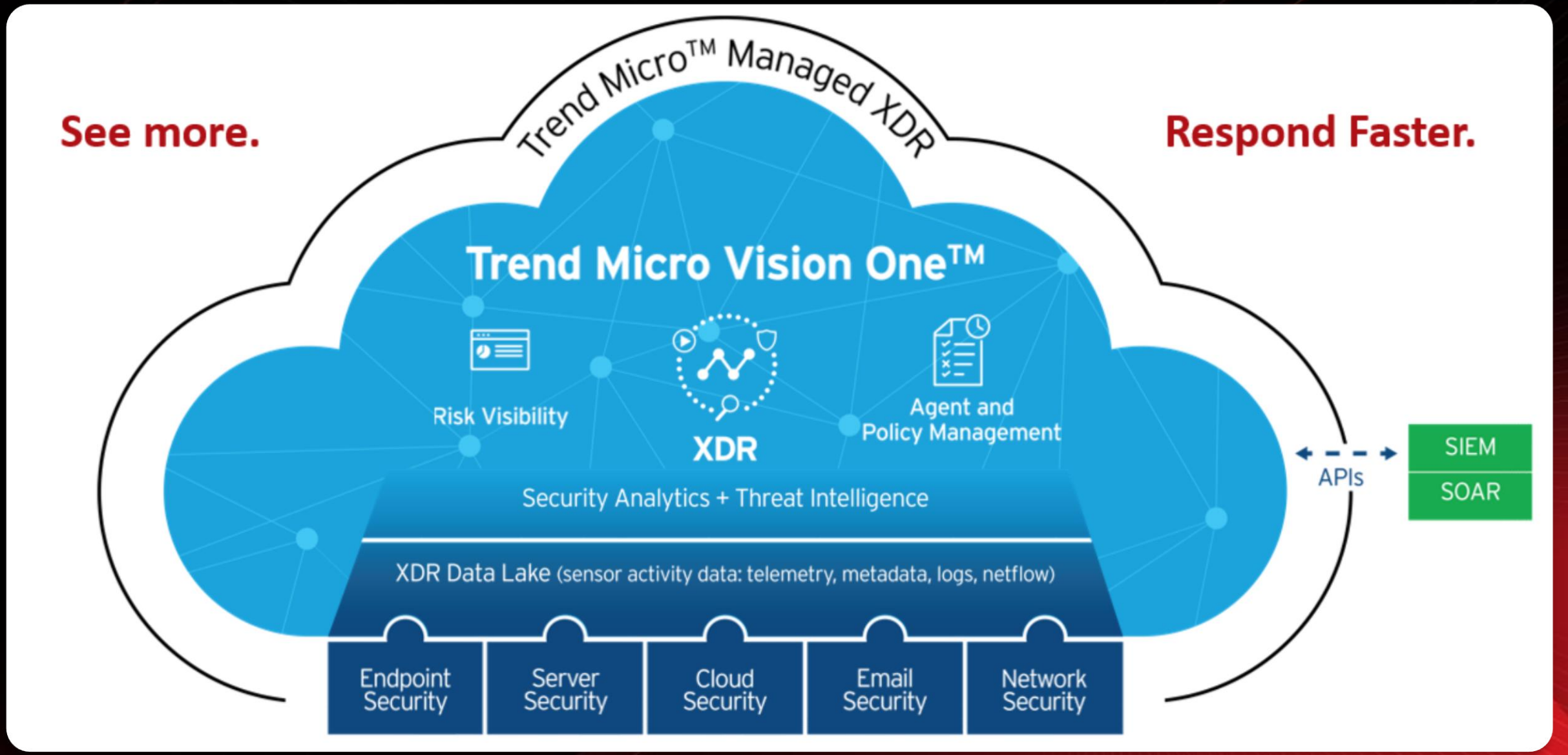
MX Record

Software

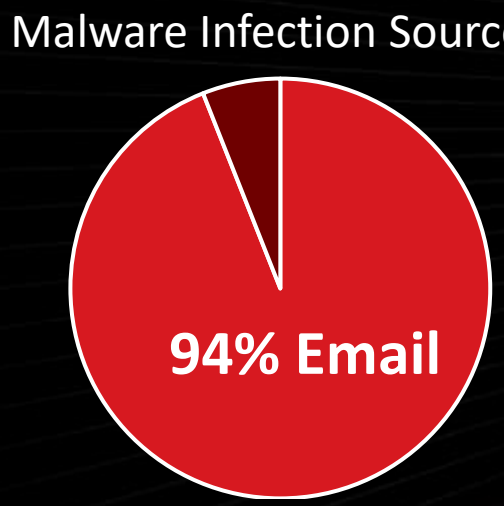
User settings

Web proxy

TREND MICRO


See more.
Respond Faster.
Trend Micro™ Managed XDR
Trend Micro Vision One™
Risk Visibility
XDR
Agent and
Policy Management
Security Analytics + Threat Intelligence
XDR Data Lake (sensor activity data: telemetry, metadata, logs, netflow)
Endpoint Security
Server Security
Cloud Security
Email Security
Network Security
APIs
SIEM
SOAR

Por qué añadir XDR al correo electrónico



Datos de la actividad :

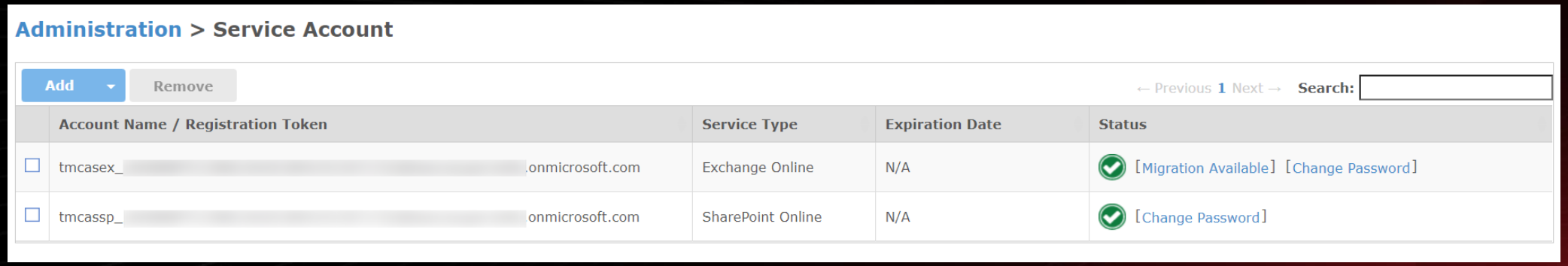
- Metadatos de los mensajes (correo electrónico externo + interno))
- Metadatos adjuntos
- Enlaces externos
- Actividad de los usuarios (logins)

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

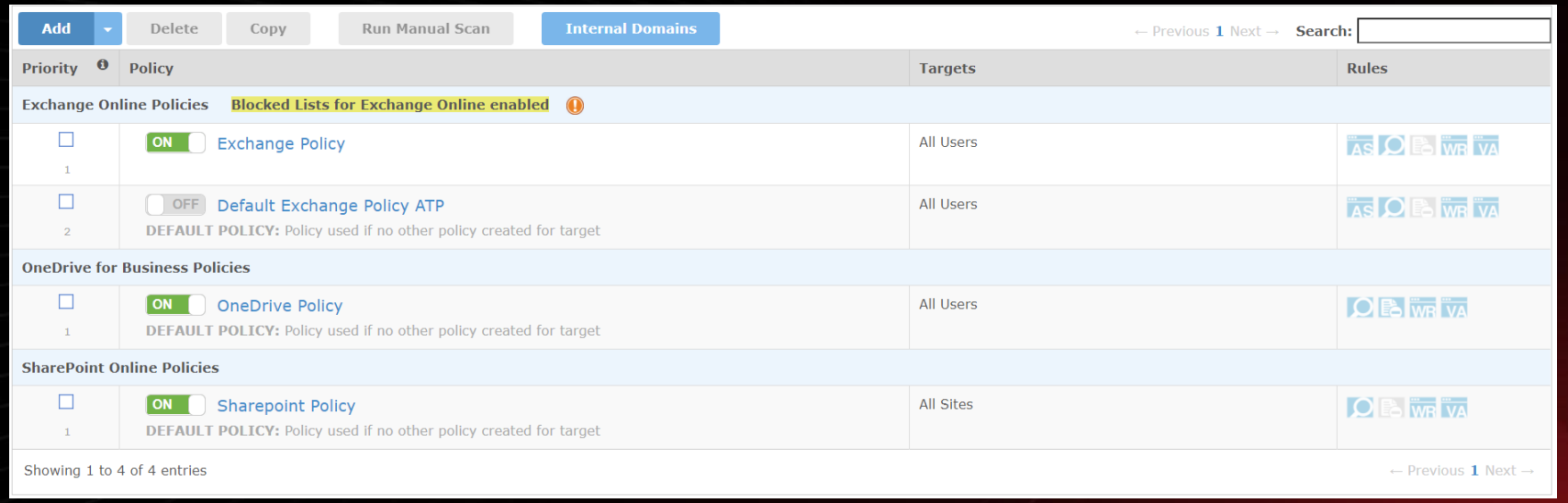
Investiga: ¿Quién más ha recibido este correo electrónico/amenaza?

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

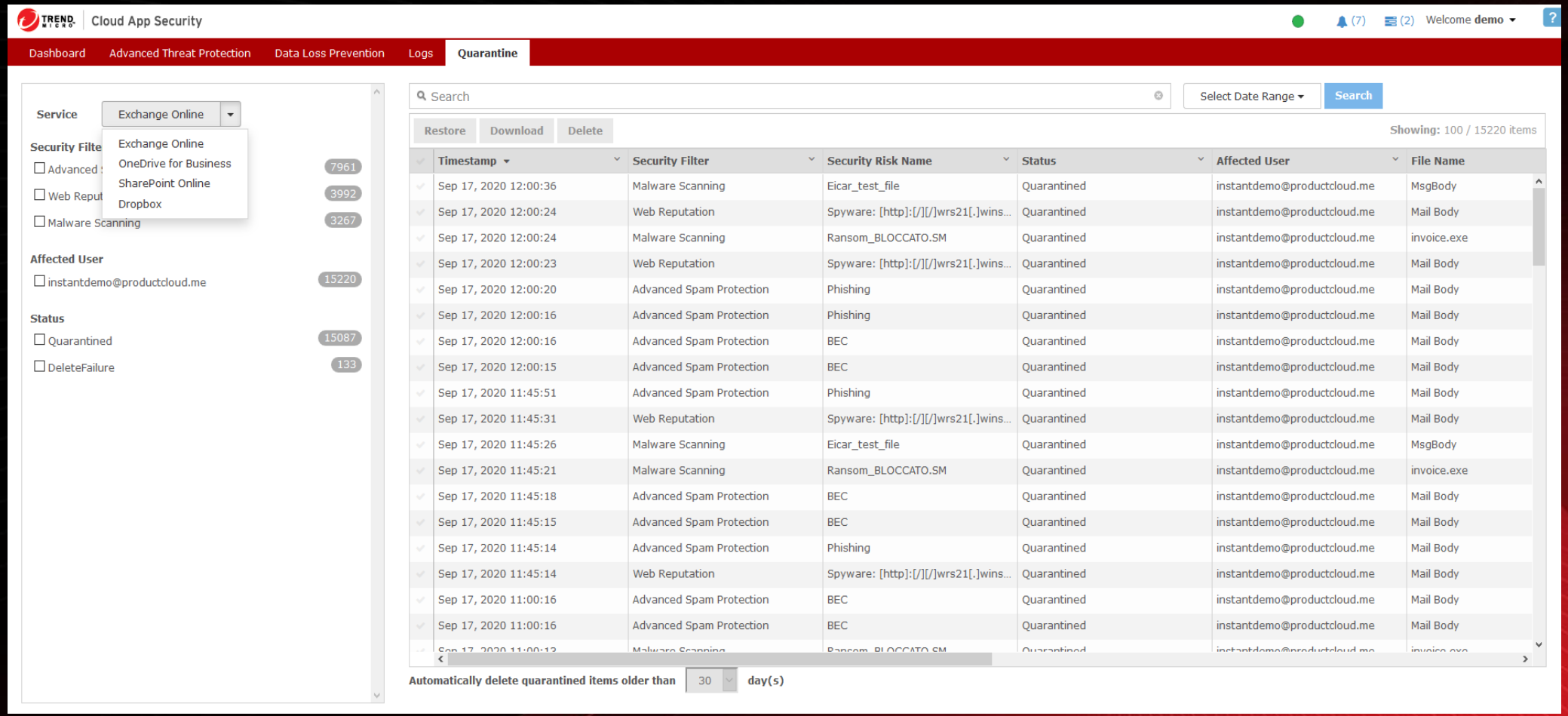
Service Account Integration



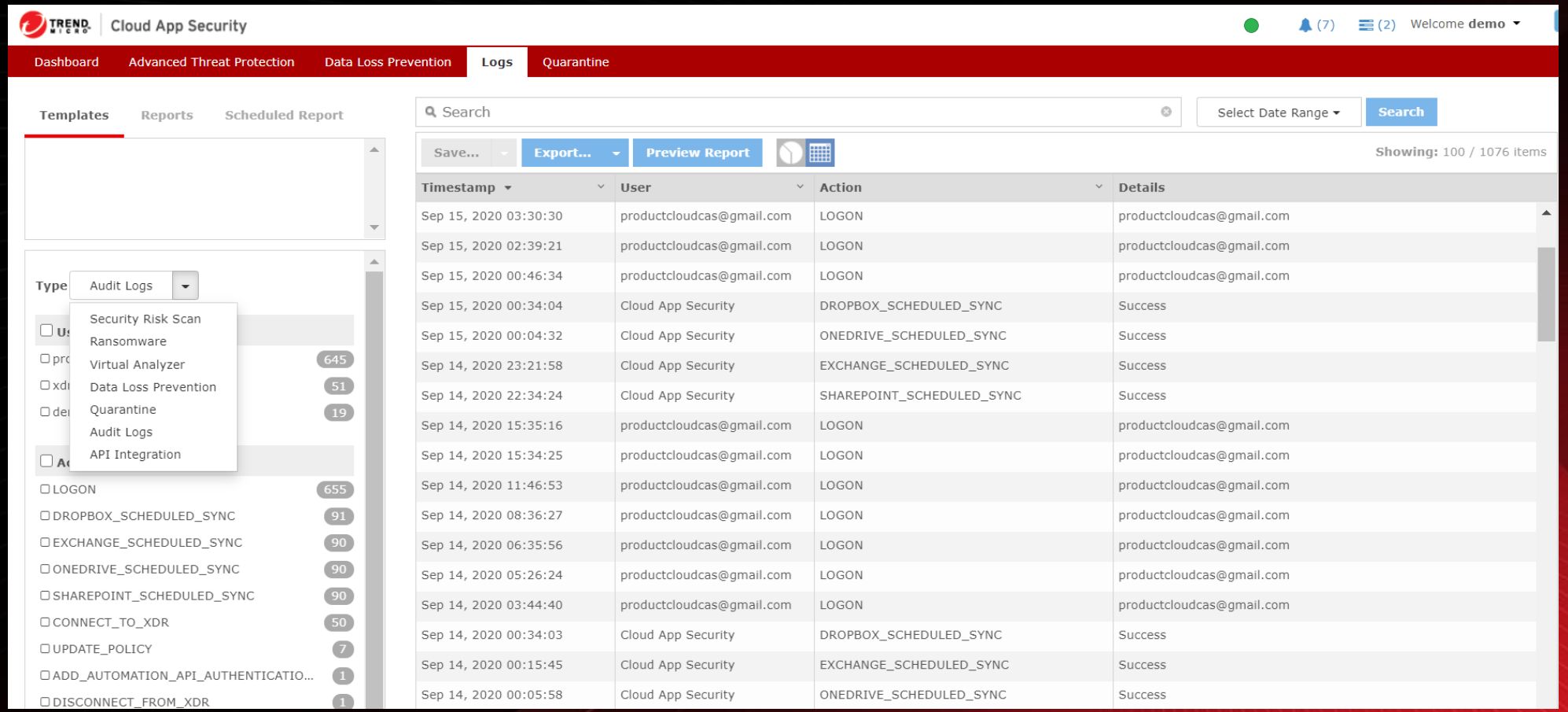
Policy Configuration



Quarantine



Logs & Reporting




TREND MICRO
DEMOS

Actividad:

Reconocimiento de Phishing

https://phishingquiz.withgoogle.com/

¡Muchas Gracias!

TREND MICRO™