Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Endpoint Security
Breakout Session

El equipo

Endpoint Security

- Alejandro Garcia
- Fernando Segura
- David Nieto
- Julio Quintero

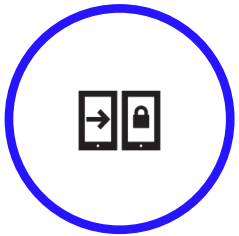
Trellix

Antes de comenzar

Use the following WIFI:
SID: **to_be_defined**
Password: **to_be_defined**

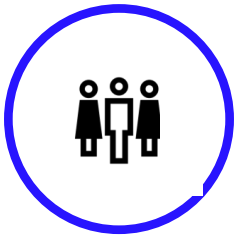
Ponga atención a las siguientes instrucciones....

Silenciar los teléfonos



Silencie o apague sus teléfonos inteligentes y otros dispositivos electrónicos para minimizar las distracciones durante la presentación.

Baños



Los baños se encuentran antes de la recepción a su derecha.

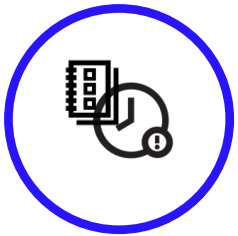
Salidas de emergencia

Familiarícese con las salidas de emergencia más cercanas, ubicadas justo antes de la recepción a su izquierda. En caso de emergencia, siga las señales de salida y diríjase con calma a la salida más cercana.

Q&A

Tendremos una sesión de preguntas y respuestas al final de la presentación. Por favor, guarde sus preguntas hasta entonces.

Horarios



Se espera que la sesión dure aproximadamente
3 horas con un descanso de 30 min.

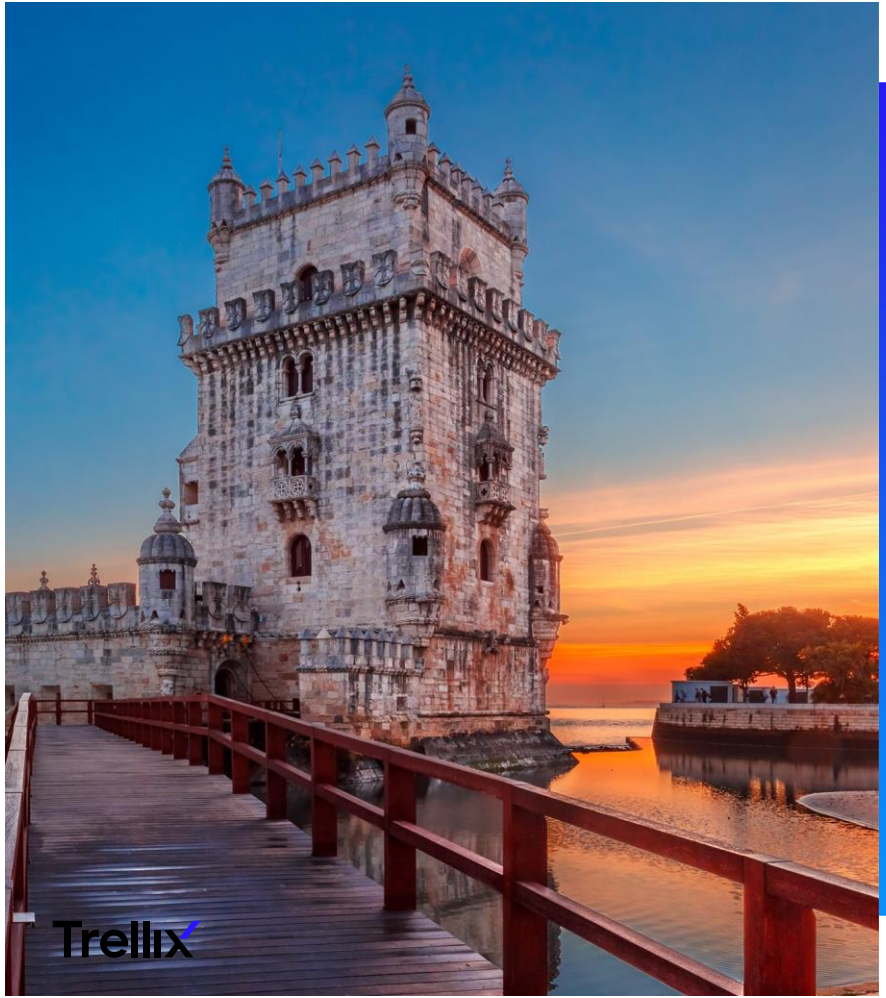
Trellix

Trellix

Endpoint Forensics (HX)

EMEA & LTAM
Partner Tech Summit

October, 2024

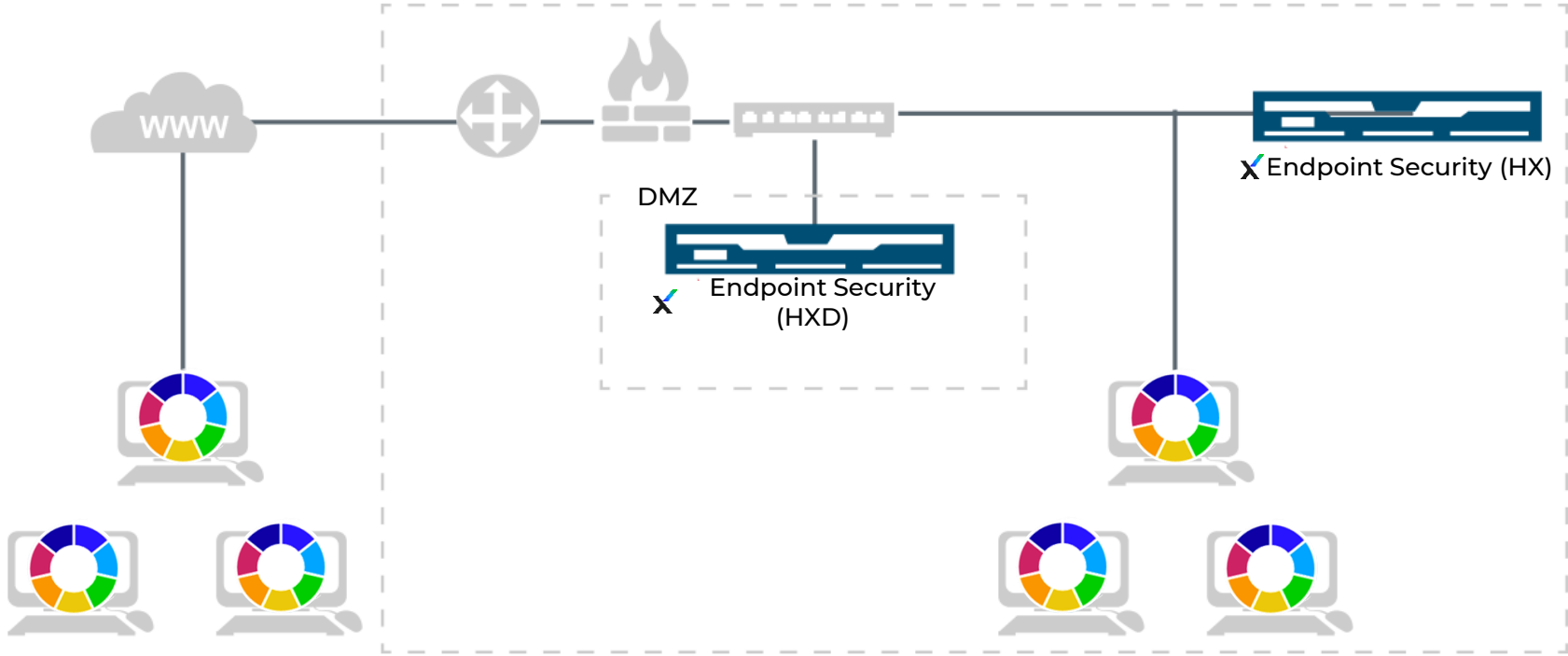


Agenda

Endpoint Security

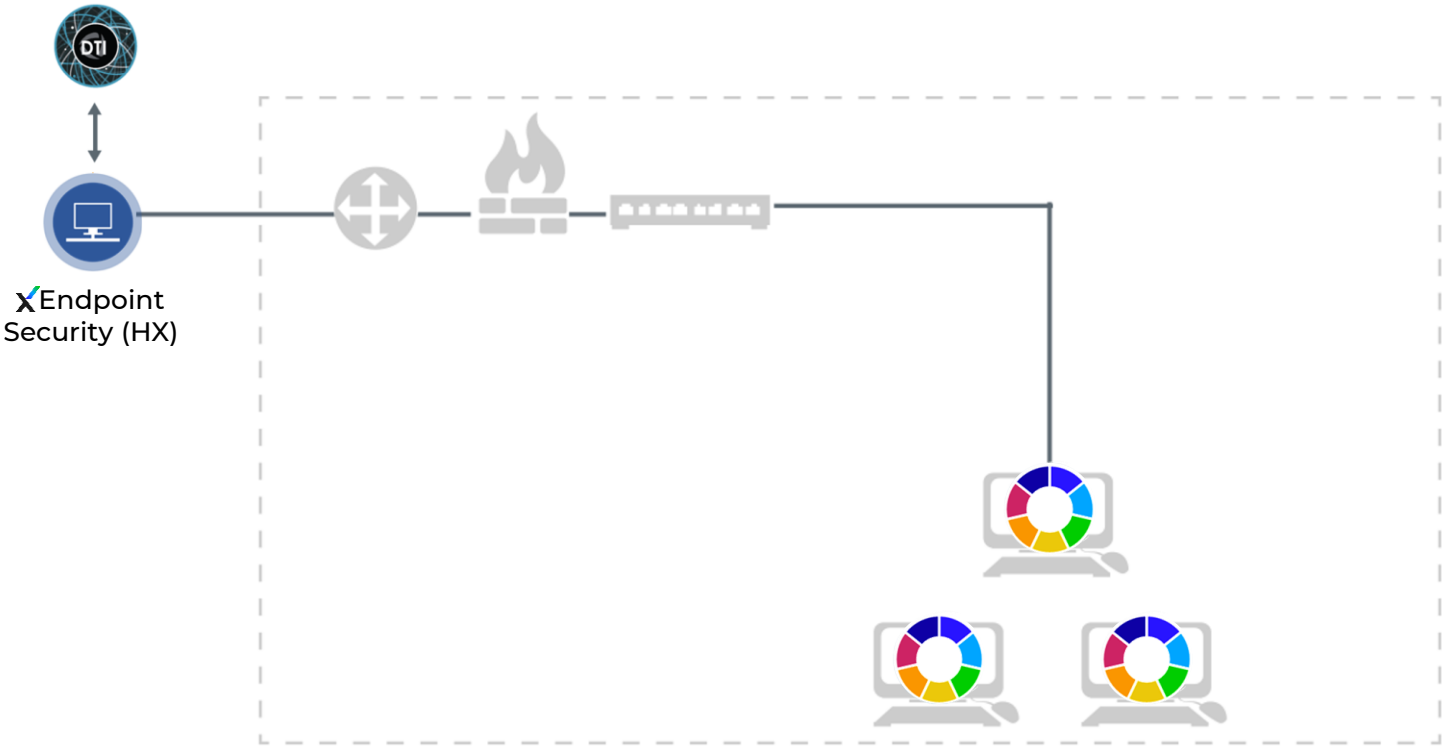
- Despliegue
- Checklist de administración
- Licenciamiento
- DTI
- Actualizaciones
- Usuarios y roles
- Backups
- Alertas
- Comandos
- Administración

Despliegue: On-Premises



Trellix

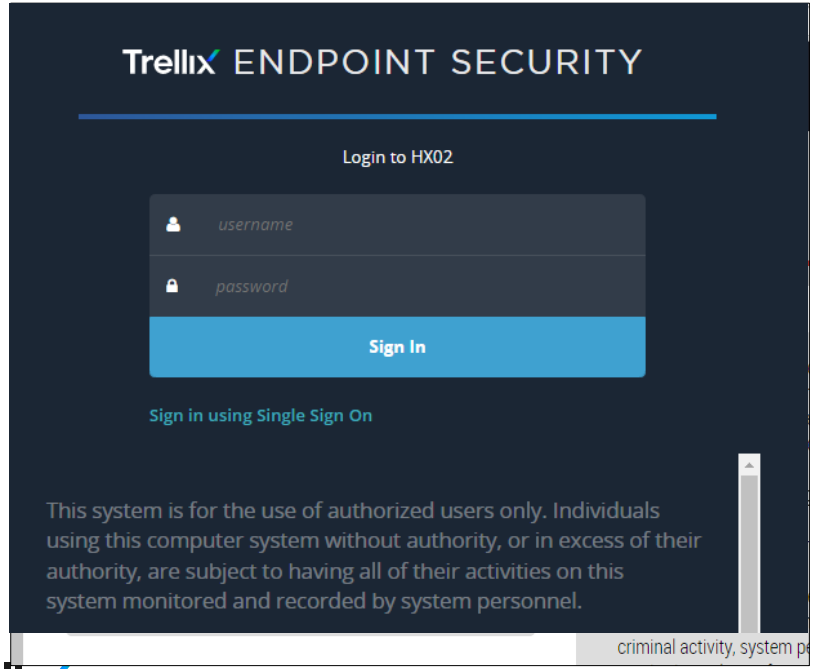
Despliegue: Cloud



Trellix

Interfaces de administración

Web UI



CLI

```
HX-TRN > enable
HX-TRN # configure term
HX-TRN (config) # confi

Fireeye configuration w

Step 1: Hostname? [HX-T
Step 2: Admin password
unchanged)?
Step 3: Use DHCP on eth
Step 4: Enable NTP? [ye
Step 5: Enable IPv6? [n
Step 6: Enable remote a
[yes]
Step 7: Product license
Step 8: Security-conten
skip)?
```

API

Trellix

Checklist de despliegue

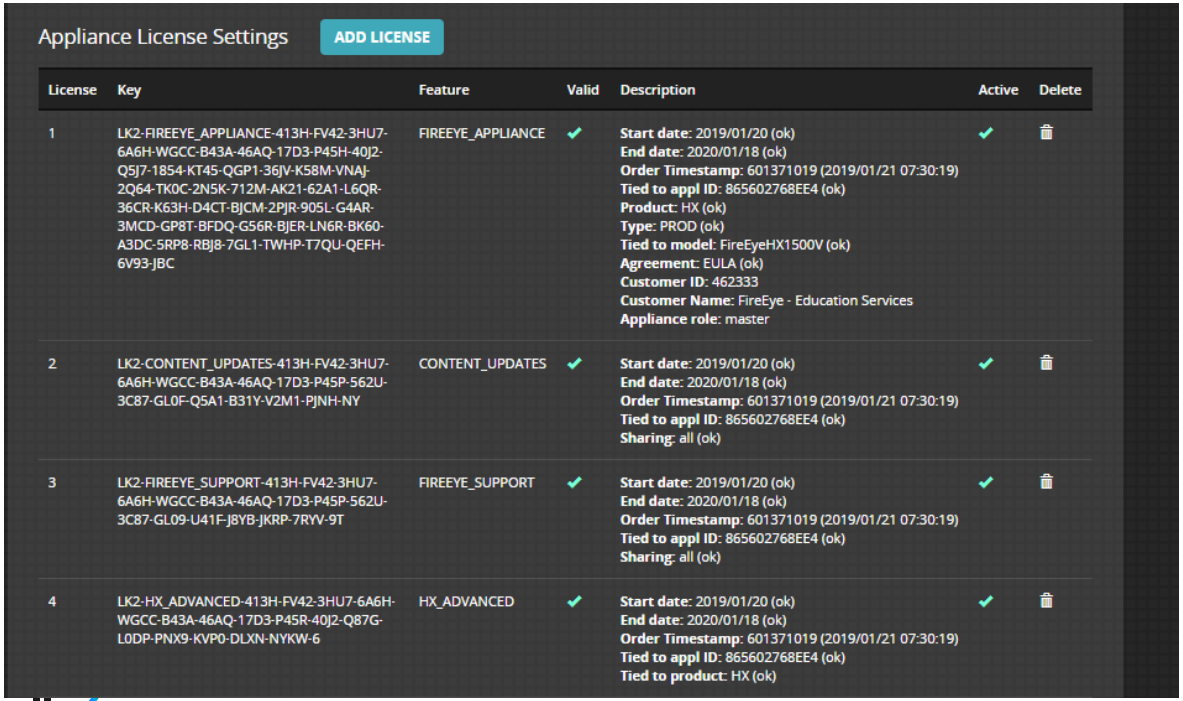
Configuración general del appliance

- Licencias
- DTI
- Updates
- Usuarios
- Backups del appliance

DMZ appliance configuration

Licencias del Appliance

Admin > Appliance Settings



Review licenses to show they are:

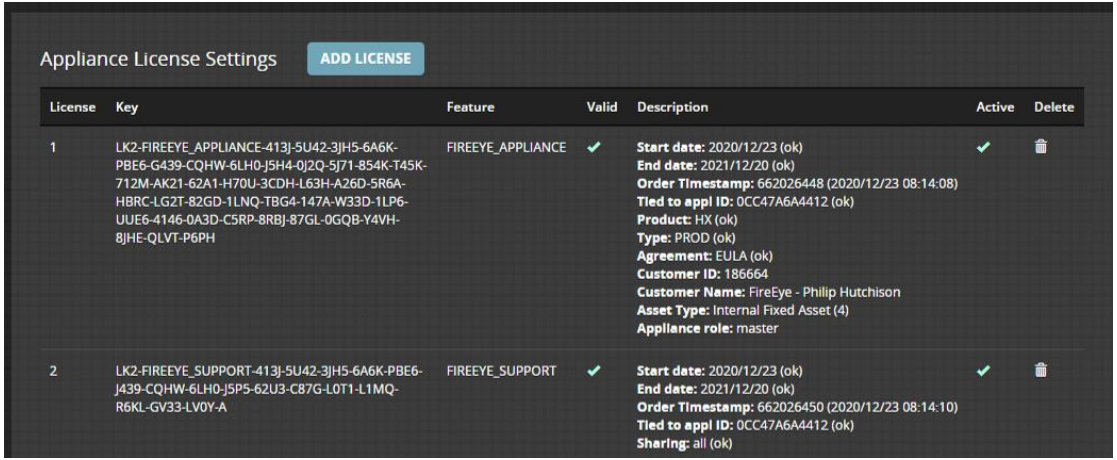
- ✔ Valid
- ✔ Active

Trellix

Tipos de licencia

License Key	Description
FIREEYE_APPLIANCE	Necesario para registrar el sistema y utilizar las funciones del producto.
FIREEYE_SUPPORT	Permite que su sistema reciba actualizaciones de imágenes de software y las últimas imágenes de invitados.
CONTENT_UPDATES	Permite que su sistema acceda a la red Dynamic Threat Intelligence (DTI), que proporciona la inteligencia más reciente sobre ciberataques avanzados y destinos de devolución de llamada de malware. Esto permite que los productos de Trellix reconozcan de forma proactiva nuevas amenazas y bloqueen los ataques. • La configuración más común es la licencia de uso compartido bidireccional. • La licencia de uso compartido unidireccional está disponible para una configuración alternativa.
HX_ADVANCED	Permite el acceso a las exhaustivas solicitudes de búsqueda empresarial, las solicitudes de adquisición de datos y las solicitudes de puntos finales de adquisición masiva de la serie HX a través de la API. Esta licencia se conoce como licencia de licencia de Endpoint Security Power.

Aplicar Licencias



Para instalar licencias:

1. Click **Admin > Appliance Settings.**
2. Click **Appliance Licenses.**
3. Click **Add License.**
4. Pegue la clave de licencia que obtuvo de Trellix en el cuadro Clave de licencia.

Trellix

Licensing Service

El servicio de licencias descarga automáticamente sus licencias de la red DTI y las instala.

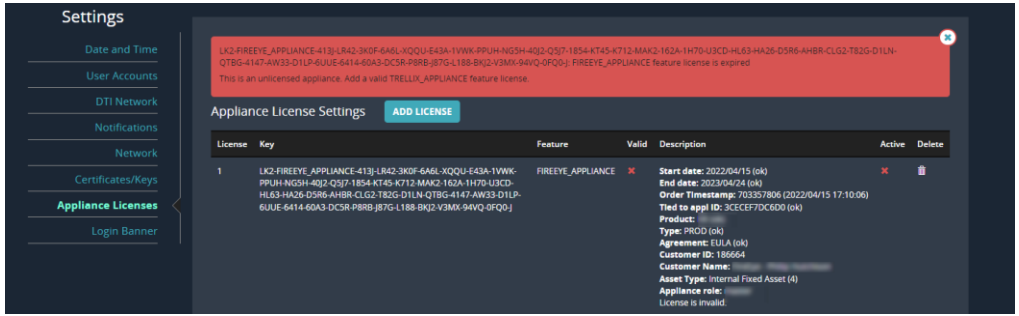
- Las licencias de los dispositivos físicos están vinculadas a la dirección Mac y al ID del dispositivo.
- Las licencias de Virtual Network Security Server se obtienen mediante tokens y un código de autenticación.

```
hostname (config) # show fenet license
fenet License Update Service

Licensing service: Administratively
enabled

Last time licensing service was
contacted: 2020/04/03 10:50:04
Last time licensing service was
contacted successfully: 2020/04/03
10:50:04
Last time keys from licensing service
were applied: 2020/04/03 10:50:04
```

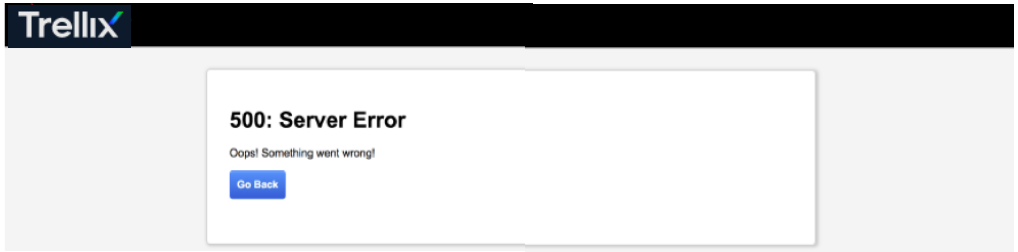
Trellix

License Issues: Síntomas

Banner



Web UI Inaccesible

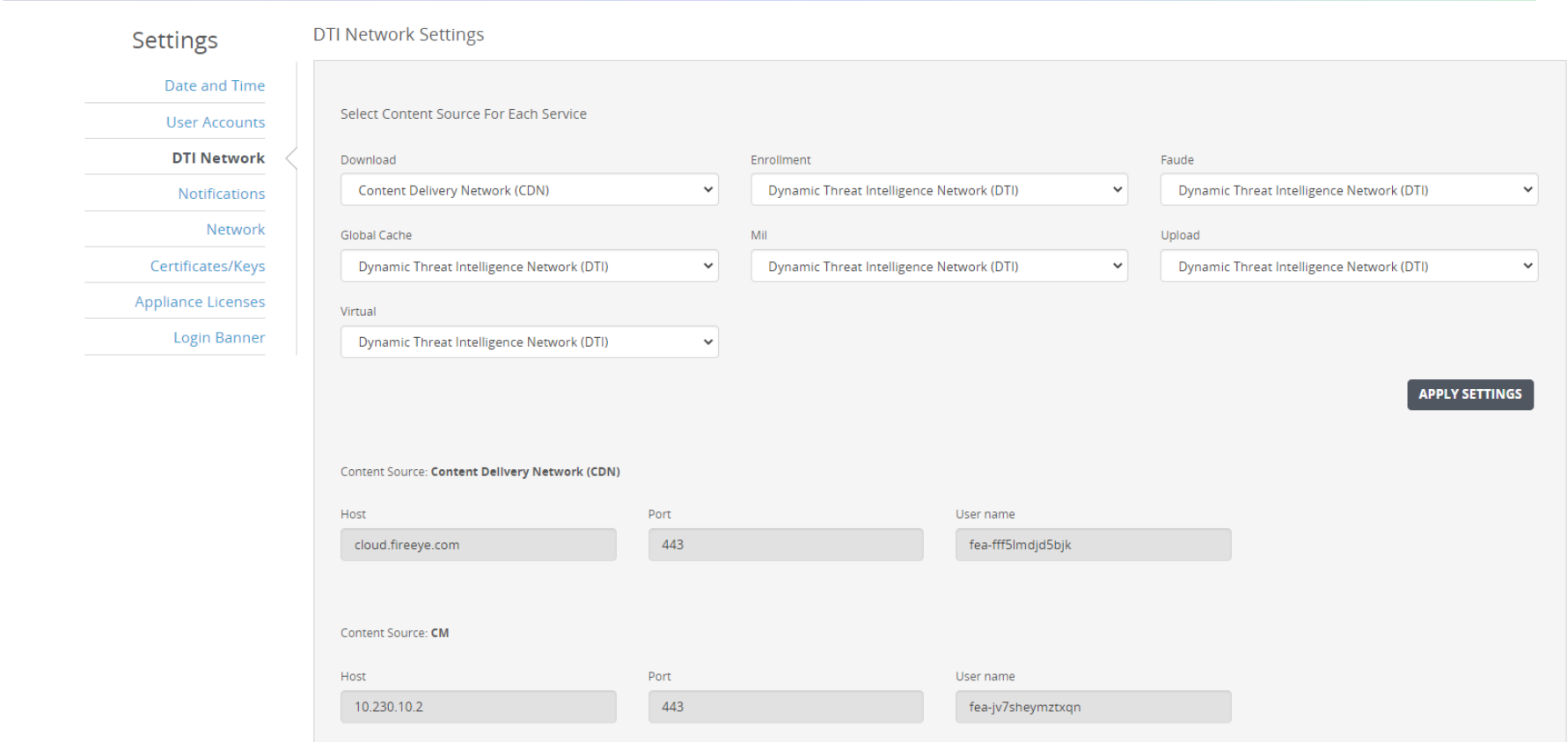


Posibles correcciones

- Servicios de Licencias
- Licencias mal formadas
- Licencias faltantes o caducadas

Trellix

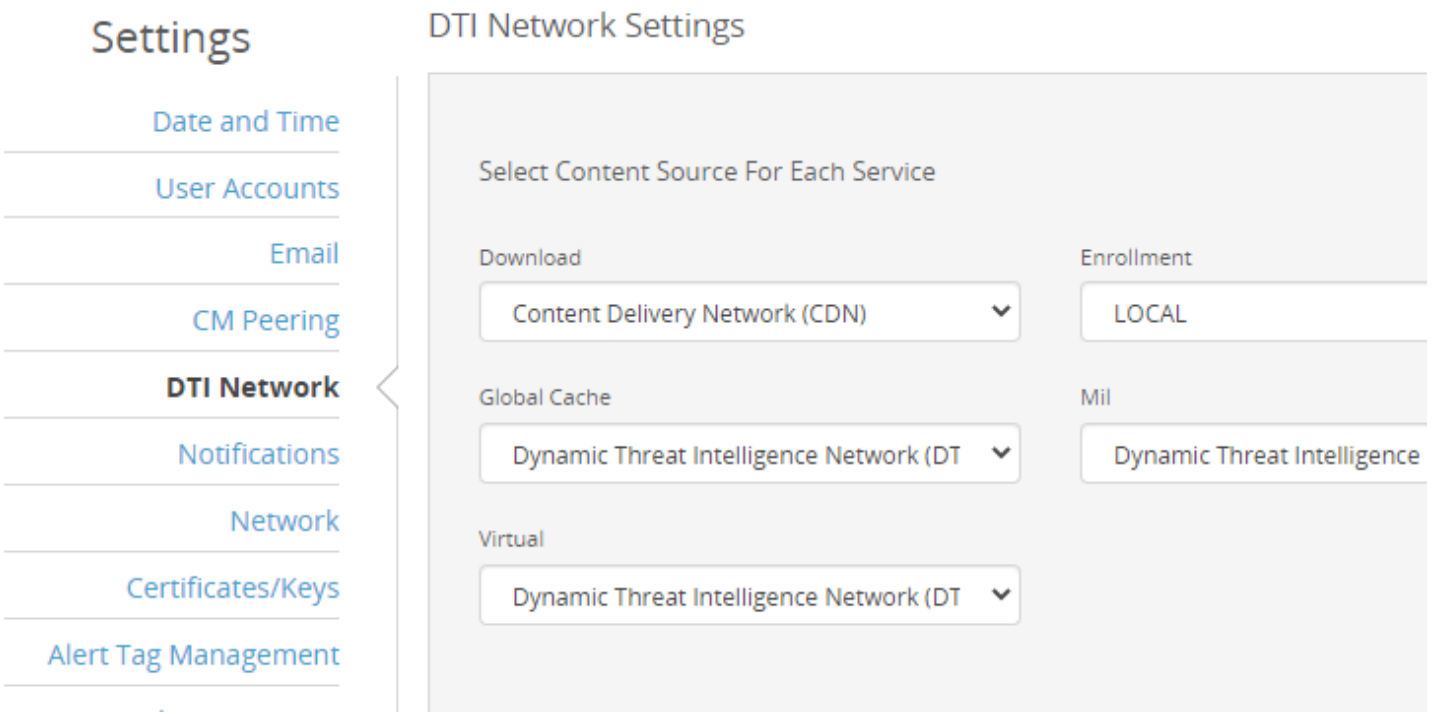
DTI Network: Configuración



DTI Services

DTI Services	Description
Download Source	El origen de las actualizaciones de software (sistema operativo y contenido de seguridad)
Upload destination	El destino de la telemetría del dispositivo y las estadísticas sanitizadas
AV-Suite	El destino para almacenar los veredictos de objetos maliciosos y no maliciosos en el servicio de detección basado en la nube de AV-Suite
Helix	El destino de las estadísticas de estado de los dispositivos habilitados para Helix
Virtual	El destino de los servicios de dispositivos virtuales, como las renovaciones de tokens de licencia y el sistema

Fuente de contenido DT



Trellix

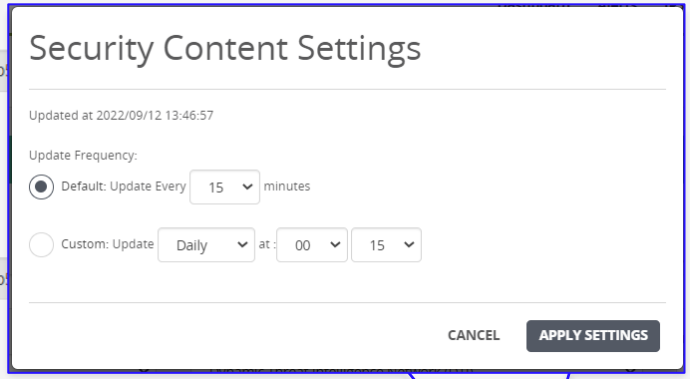
Actualización de contenido de seguridad

Content Source: **Content Delivery Network (CDN)**

Host: cloud.fireeye.com | Port: 443 | User name: fev-aylpbr4agfp

Content Source: **Dynamic Threat Intelligence Network (DTI)**

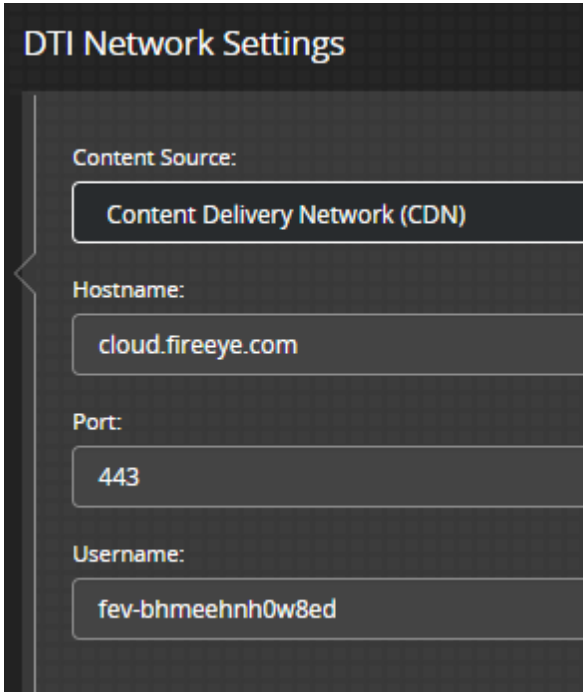
Host: staticcloud.fireeye.com | Port: 443 | User name: fev-aylpbr4agfp



Service Type	Notify	Version	Scheduled	Last Update	TimeStamp (UTC)	Settings
Security Contents	☐	1300.112	For every 15 minutes	2022/09/12 13:46:57	2022-09-12 12:10:00	Auto update enabled: true Update Frequency: every 15 minutes

Trellix

Revisión de la configuración de DTI (Fenet settings)




```
host-4f9836 (config) # show fenet dti configuration

DTI CLIENT CONFIGURATIONS:

 APPLIANCE SETTINGS:

  Appliance ID       : 86406B7B9D85

 ACTIVE SETTINGS:

  Mode               : online
  Download source    : CDN (fev-bhmeehnh0w8ed@cloud.fireeye.com)
  Upload destination : DTI (fev-bhmeehnh0w8ed@up-
cloud.fireeye.com)
  Mil service        : DTI (fev-bhmeehnh0w8ed@mil-
cloud.fireeye.com)
  Faude service      : DTI (fev-bhmeehnh0w8ed@unity.fireeye.com)
  Virtual service    : DTI (fev-bhmeehnh0w8ed@cloud.fireeye.com)
  AVSuite service    : DTI (fev-bhmeehnh0w8ed@unity.fireeye.com)
  Helix service      : DTI (fev-bhmeehnh0w8ed@helix.fireeye.com)

 ACTIVE SETTINGS FOR HTTP PROXY:
```

Trellix

Problemas comunes de DTI

1. Problema de conexión.

   Acción: Confirme la conexión con el servicio DTI en la nube mediante telnet.

```
4f98-TRN (config) # telnet cloud.fireeye.com 443

Trying 162.159.246.125...
Connected to cloud.fireeye.com.
Escape character is '^]'.
```

2. Problema de autenticación.

   Acción: Confirmar credenciales.

Trellix

Configuración de Fenet: comandos

Cambiar la dirección del servicio

fenet dti source type DTI address <address you are using> port 443
fenet dti source default DTI

fenet dti upload destination type DTI address up-<address you are using> port 443
fenet dti upload destination default DTI

fenet dti enrollment service type DTI address <address you are using> port 443
fenet dti enrollment service default DTI

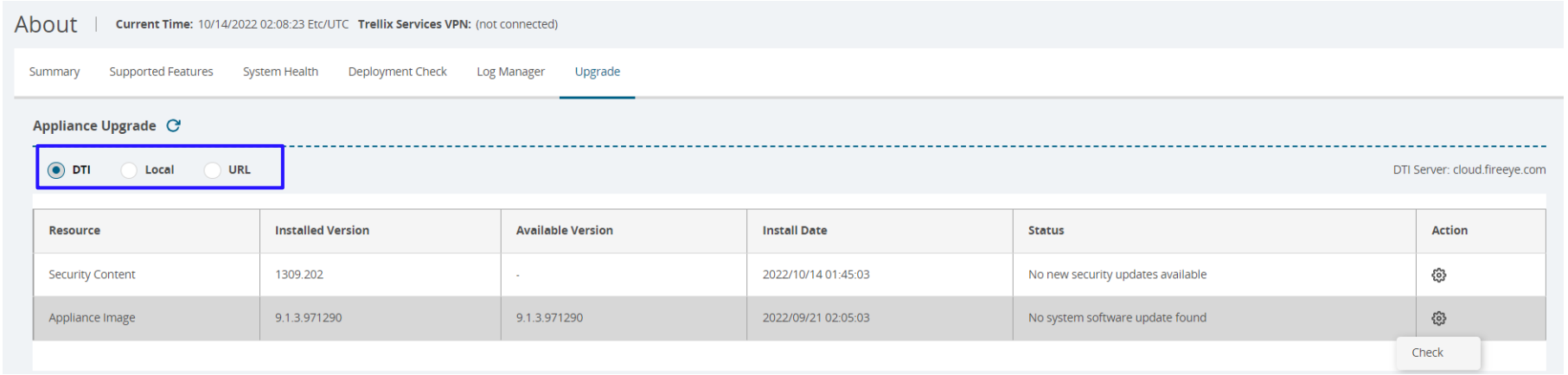
fenet dti mil service type DTI address mil-<address you are using> port 443
fenet dti mil service default DTI

fenet dti virtual service type DTI address <address you are using> port 443
fenet dti virtual service default DTI

Establecer el tipo de servidor predeterminado para el servicio (CDN o DTI)

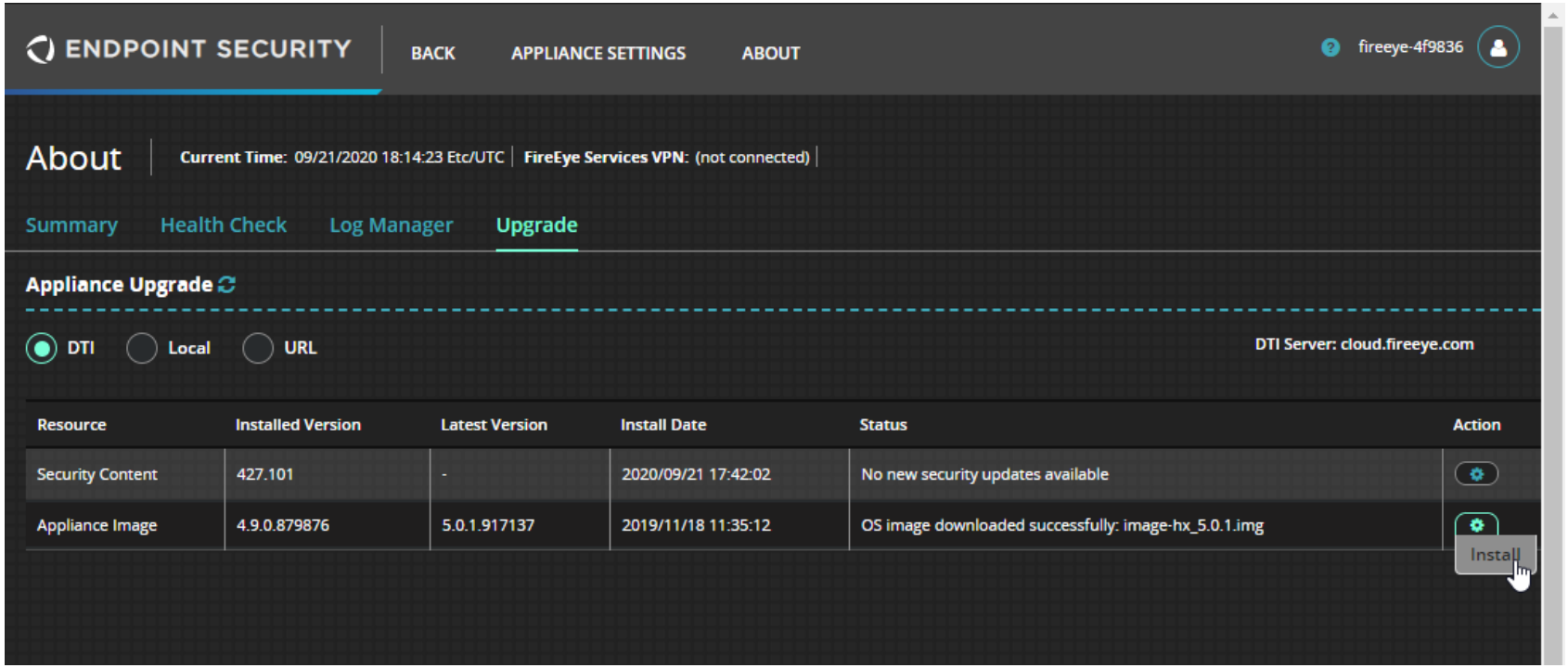
Trellix

Fuentes de actualización del Appliance



Trellix

Proceso de actualización



Trellix

Tipos de actualización

Update Type	Frequency	Description
Security Content	Cada hora	Las actualizaciones de contenido de seguridad son fundamentales para garantizar que el dispositivo Trellix esté al tanto de las amenazas más recientes.
Appliance Images	Una o dos veces al año	La imagen del dispositivo contiene el sistema operativo del dispositivo y NO contiene las imágenes de invitado utilizadas para detectar malware. Las actualizaciones de la imagen del dispositivo contienen mejoras importantes y correcciones de errores en el sistema operativo.

El rol de las particiones en las actualizaciones

Paso 1 – Descargar la actualización

Descargar paquete a la part 1

1
ACTIVE
ver 2.0

2
INACTIVE
ver 1.0

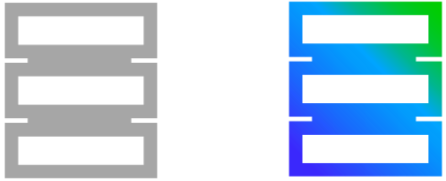
Paso 2 - Actualización en curso

1
ACTIVE
ver 2.0

2
INACTIVE
ver 3.0

Paso 3 – Aplicar la actualización

Mark for next boot



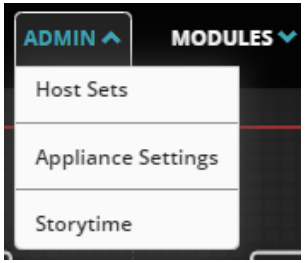
1
INACTIVE
ver 2.0

2
ACTIVE
ver 3.0

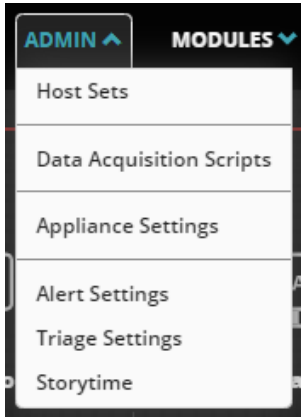
Trellix

Roles

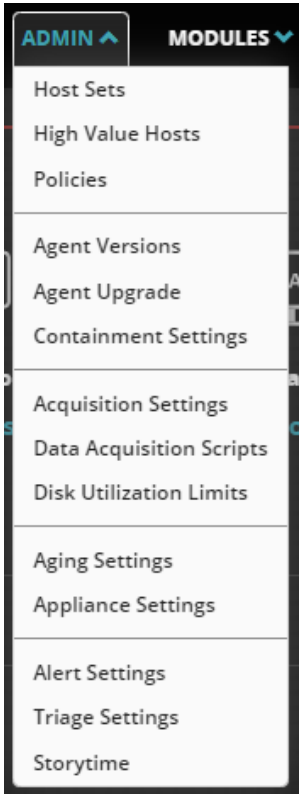
Roles más comunes:



Analyst



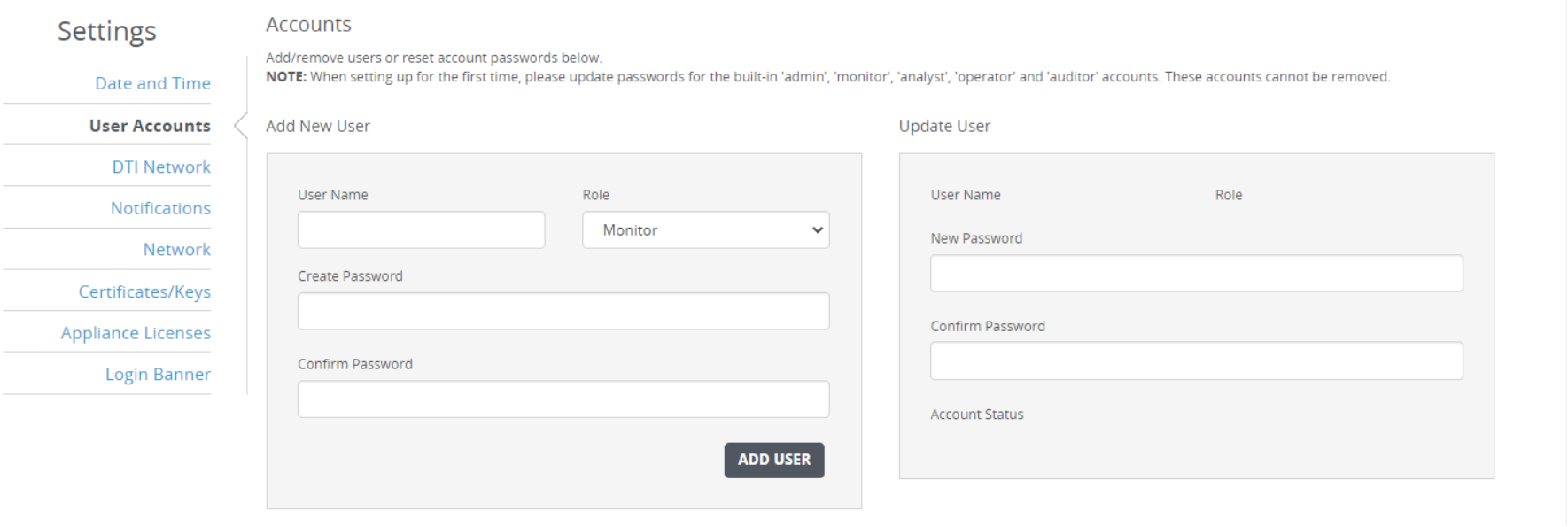
Investigator



Admin

Trellix

Cuentas de usuario



Trellix

Opciones de autenticación remota

LDAP

RADIUS

TACACS

IAM/SSO

CAC

Trellix

Tipos de copia de seguridad

Perfiles de copia de seguridad

Configuración (config) y base de datos (fedb)

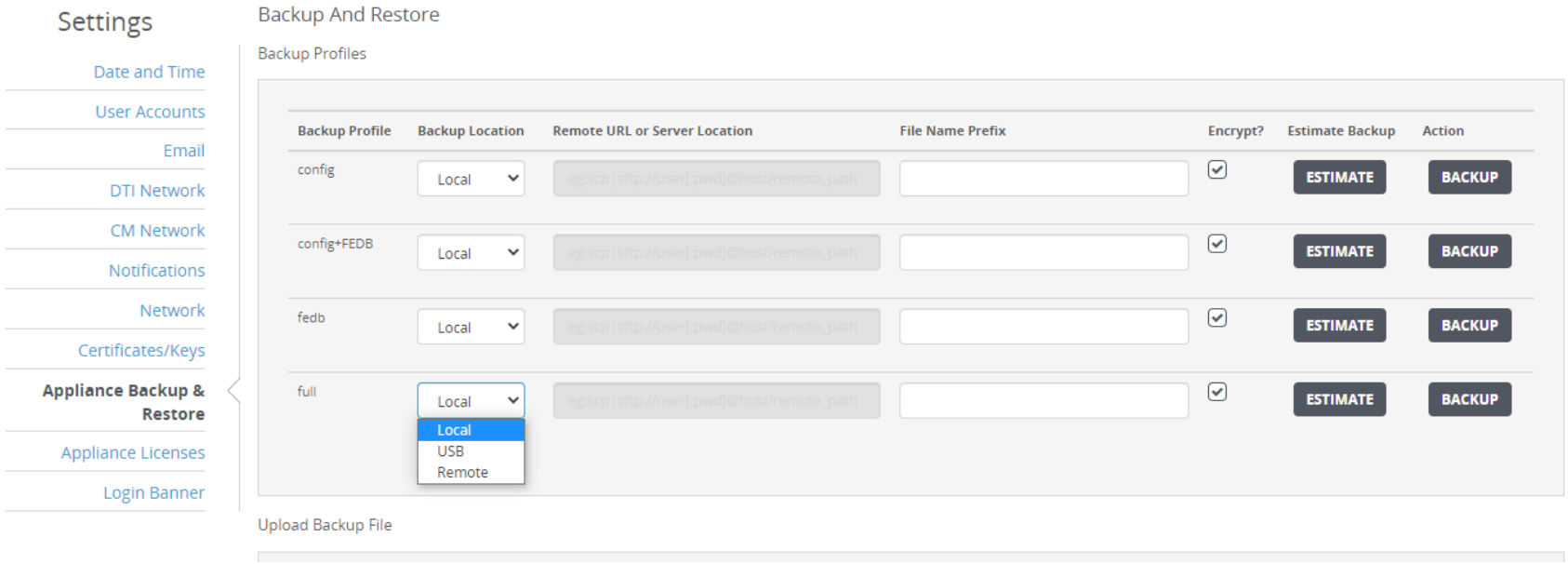
Configuración (config)

Base de datos (fedb)

Copia de seguridad completa

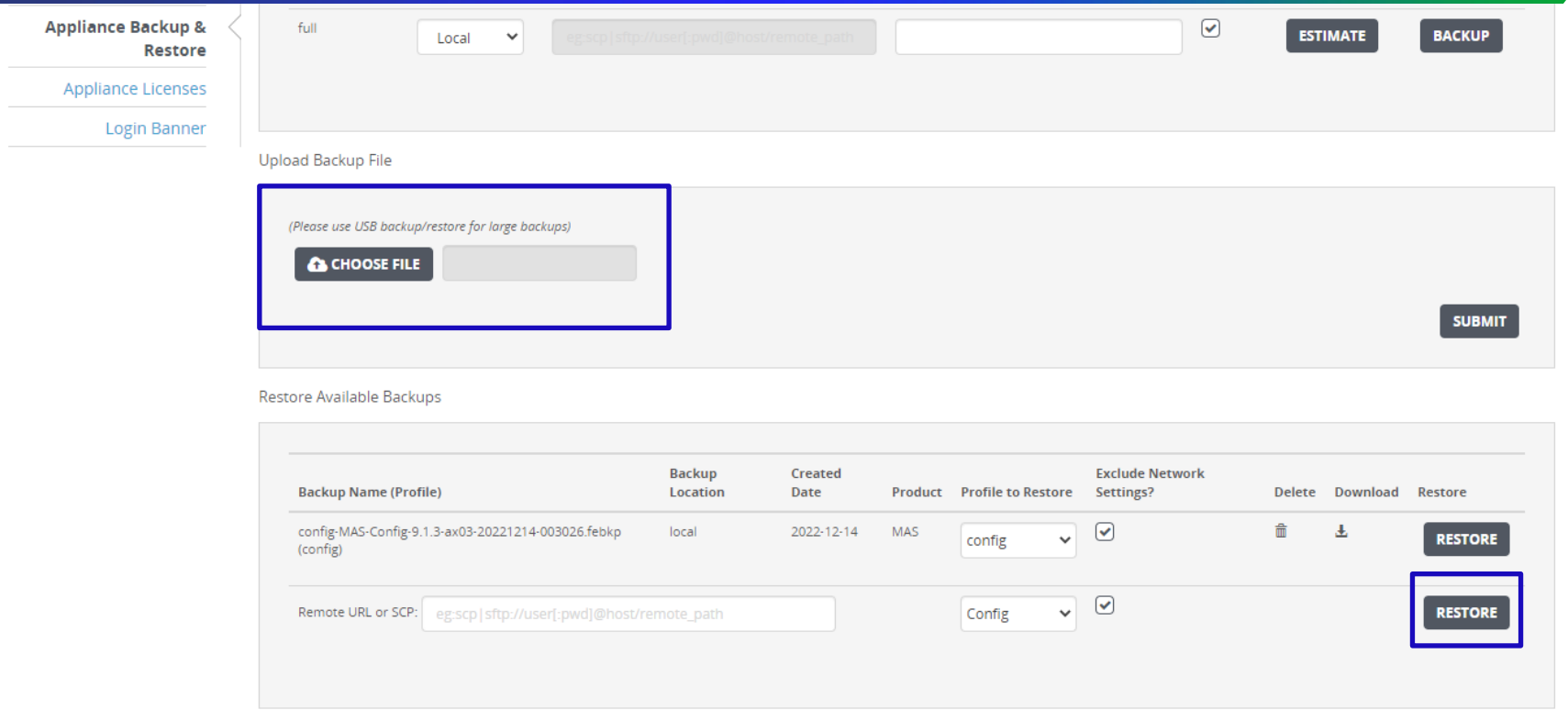
Trellix

Copia de seguridad de la base de datos



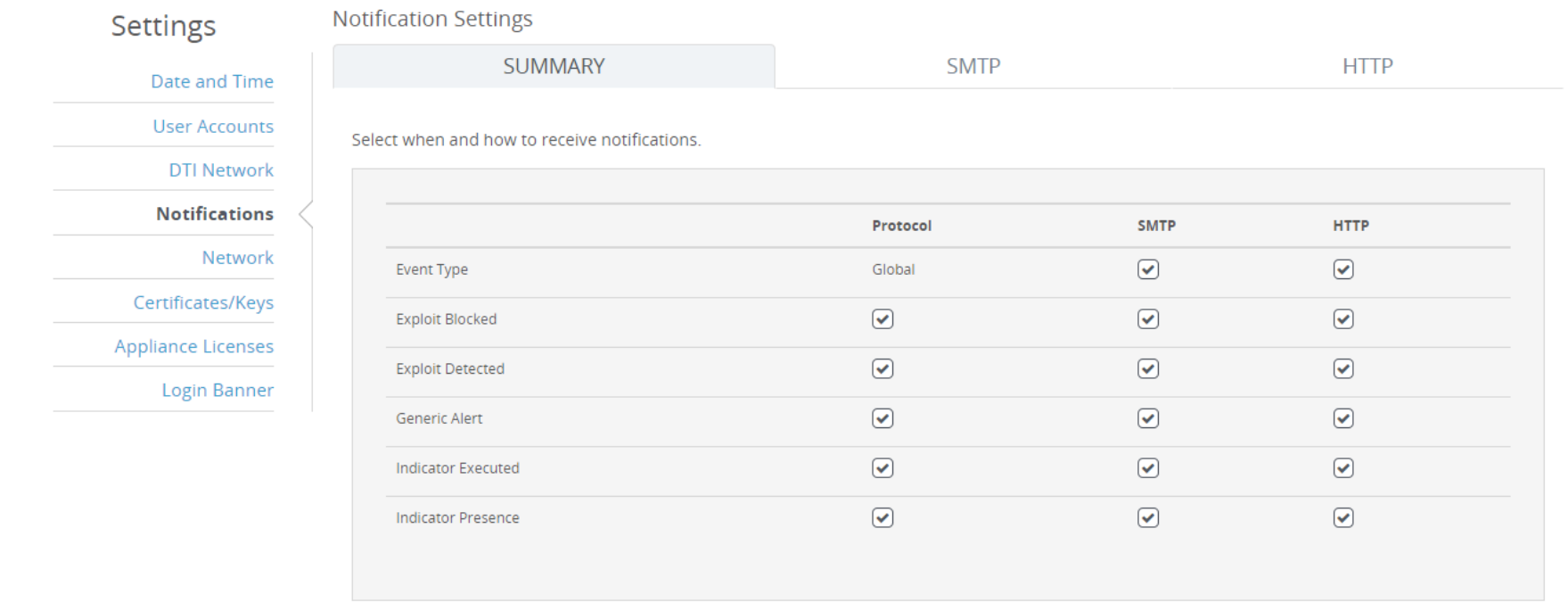
Trellix

Restauración de base de datos



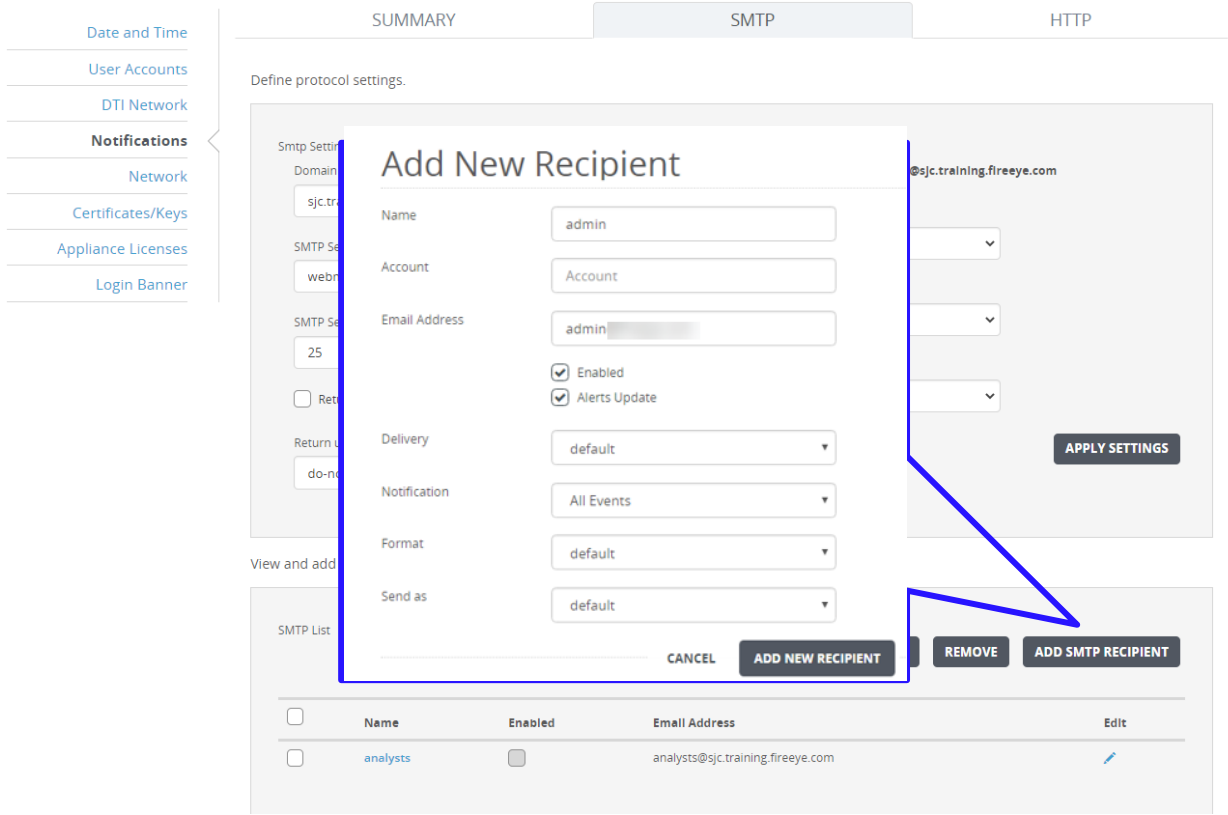
Trellix

Notificaciones de alertas



Trellix

Configuración de notificaciones SMTP



Trellix

Comandos CLI de Helix

Command	Description
helix mode (cloud)	Habilita el modo Helix; habilita automáticamente el cliente HelixConnect.
show helix	Muestra la configuración de Trellix Helix.
show helixconnect	Muestra información sobre la conexión.
show commbroker status	Muestra el estado de la conexión entre el dispositivo de seguridad de red y el módulo Comm Broker.
show commbroker health	Muestra los estados de mantenimiento del remitente del agente de comunicaciones.
show tapsender status	Muestra el estado de la conexión entre el dispositivo y la VPC de Helix.
show tapsender health	Muestra los estados de mantenimiento del módulo Recopilador de pruebas.
helixconnect troubleshoot	Comprueba la conexión con la URL de registro, el dominio y el número de puerto.

Resumen de comandos [1/2]

Command	Description
show version	Muestra información sobre la versión instalada de la imagen de arranque del dispositivo Trellix, los parches recientes, el estado de DTI, etc.
show licenses	Muestra la información de la licencia del dispositivo.
license install	Instala una nueva licencia.
license delete	Elimina una licencia actual.
show fenet license	Muestra información sobre el servicio y la actividad de actualización de licencias.
fenet license update enable	Habilita la función de actualización de licencia.
fenet license update force	Obliga a actualizar las licencias.

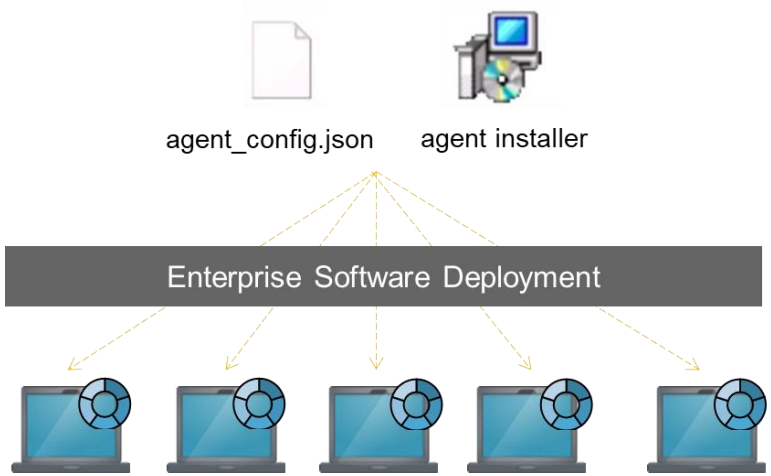
Resumen de comandos [2/2]

Command	Description
show fenet dti configuration	Muestra información sobre la configuración del servidor DTI en un dispositivo.
fenet dti source type DTI address <address you are using> port 443	Actualiza la dirección del servicio de origen de descarga de fenet* en el dispositivo.
fenet dti source default <DTI|CDN>	Establece el tipo de servidor predeterminado para el servicio de origen de descarga* en un dispositivo.
write memory	Guarda los cambios de configuración.
telnet cloud.fireeye.com 443	Comprueba la conectividad con la nube DTI.

Trellix

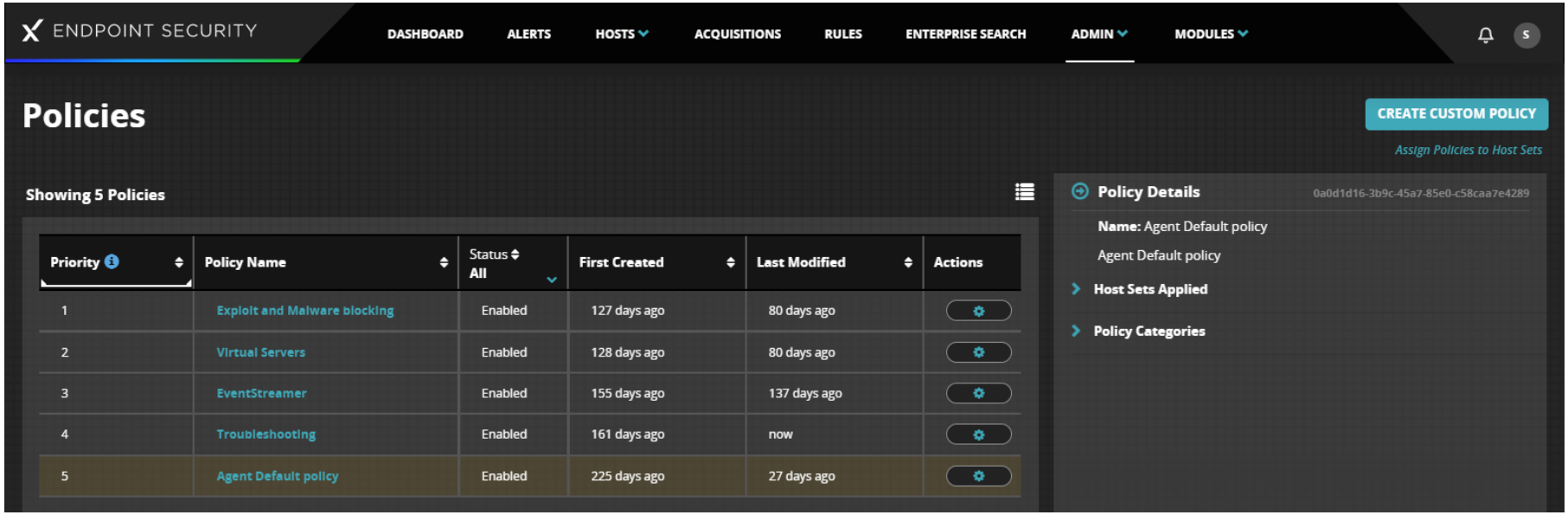
Trellix xAgent

- Peso ligero
- Proporciona cobertura para Windows, Mac y Linux
- Registra eventos del sistema en una base de datos de eventos local
- Inicia la comunicación con el controlador



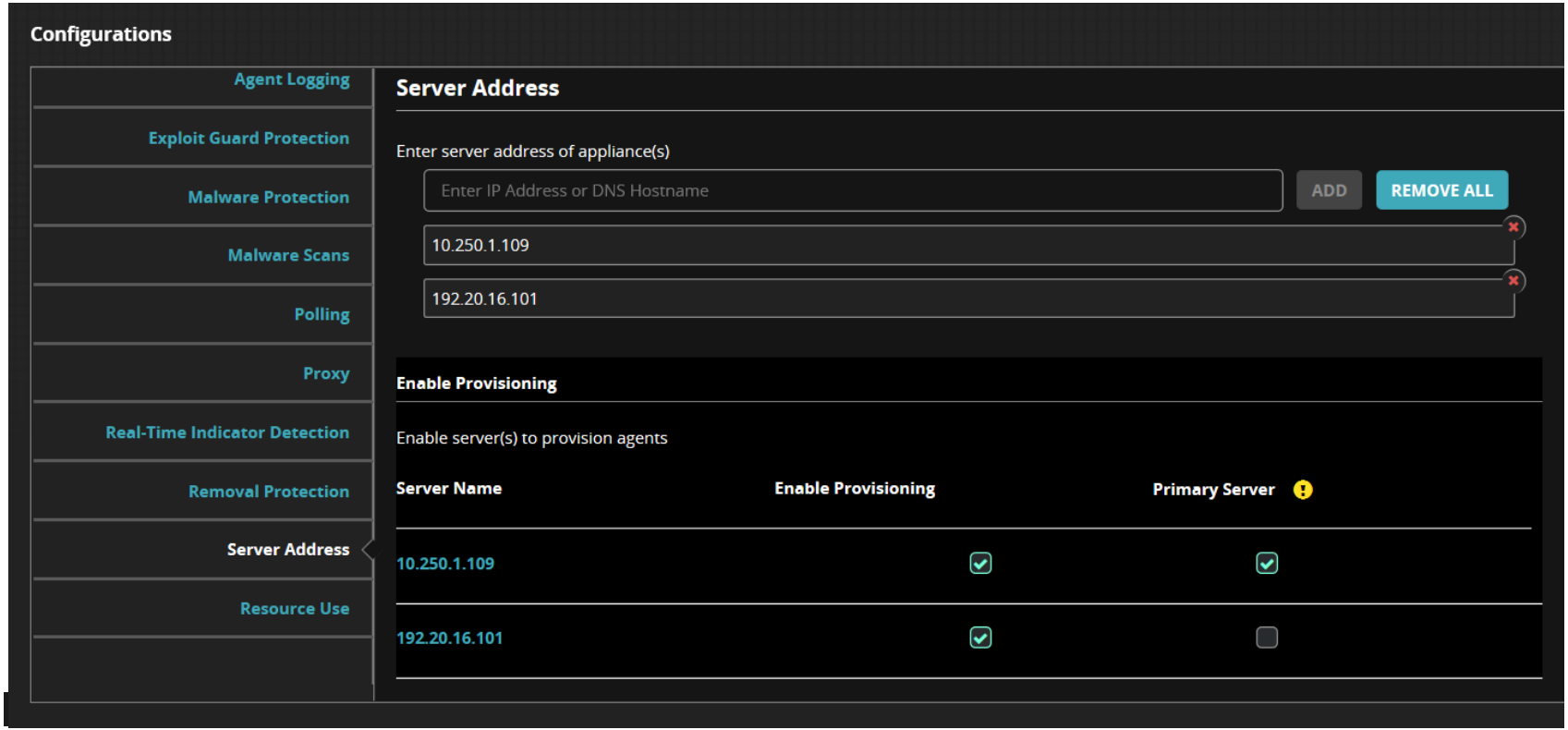
Trellix

Políticas de agentes



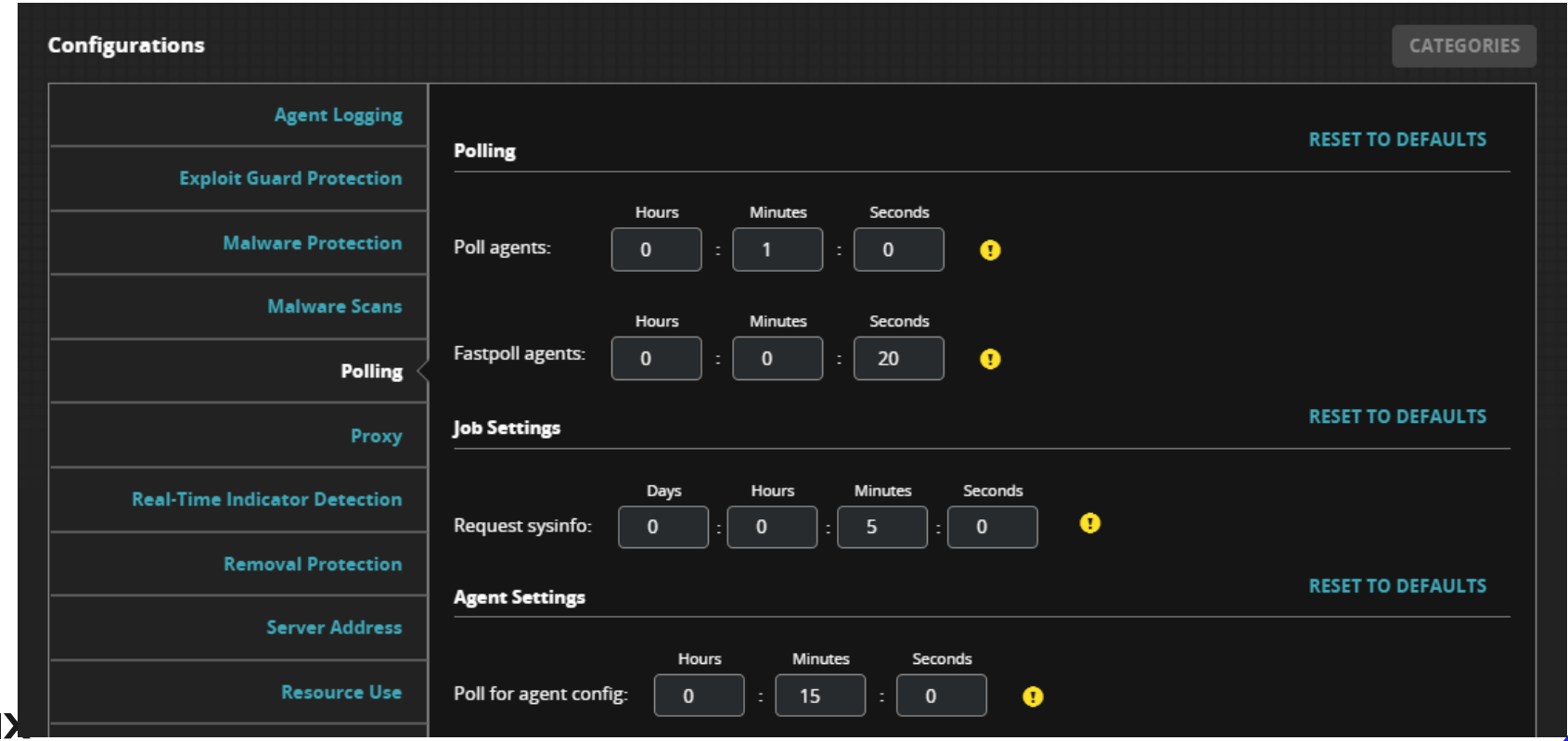
Trellix

Configuración del servidor



Trell

Políticas: Agent Polling

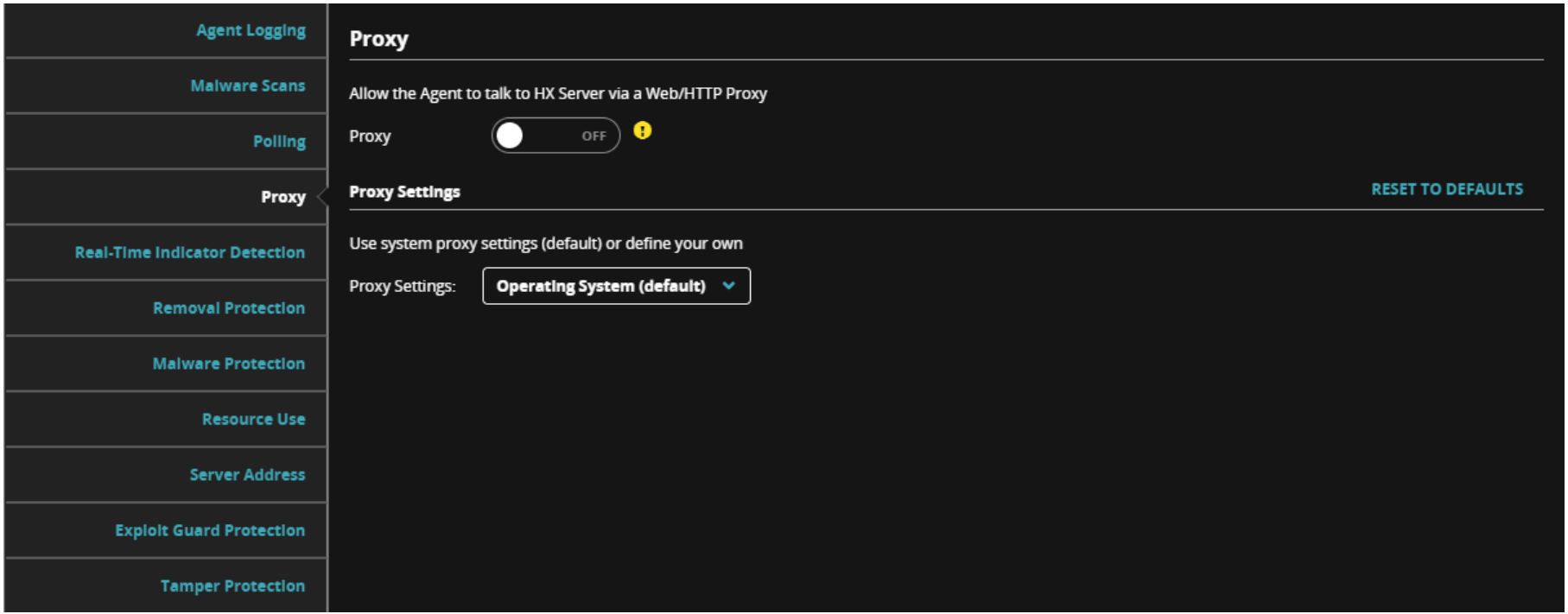


Trellix

Tipos de polling

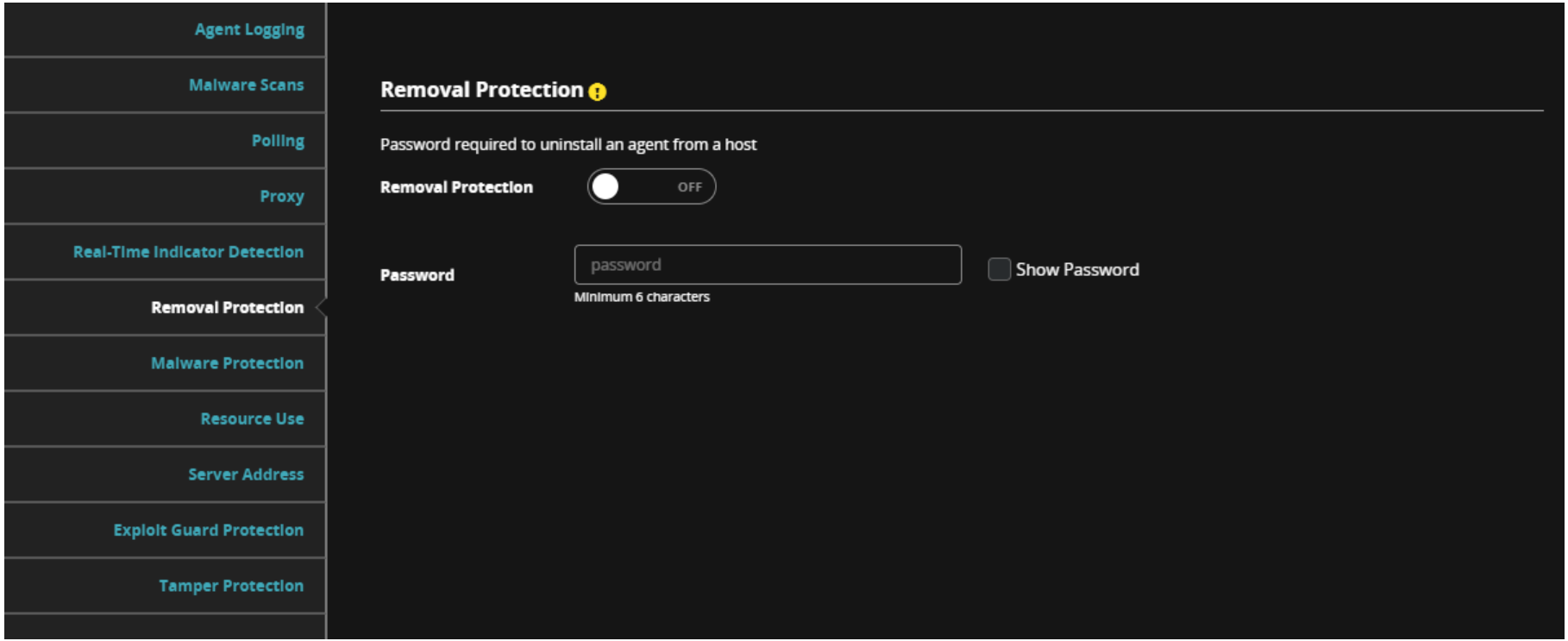
Poll Type	Description
Full	Un poll completo se utiliza para transferir información y solicitudes de tareas desde el servidor de Endpoint Security a los agentes instalados en los hosts.
Fastpoll	Fastpoll se utiliza para determinar rápidamente si se requiere un sondeo completo.
Indicator	Un poll de indicadores se utiliza para transferir los indicadores más recientes del servidor de Endpoint Security a los agentes.
Agent Configuration	Se utiliza un poll de archivo de configuración para transferir la configuración de agente más reciente desde el servidor de Endpoint Security servidor a los agentes.
Malware Detection Indicators	Se utiliza un poll de actualización de definiciones de malware para transferir las definiciones de malware más recientes al agente.

Políticas: Proxy Settings



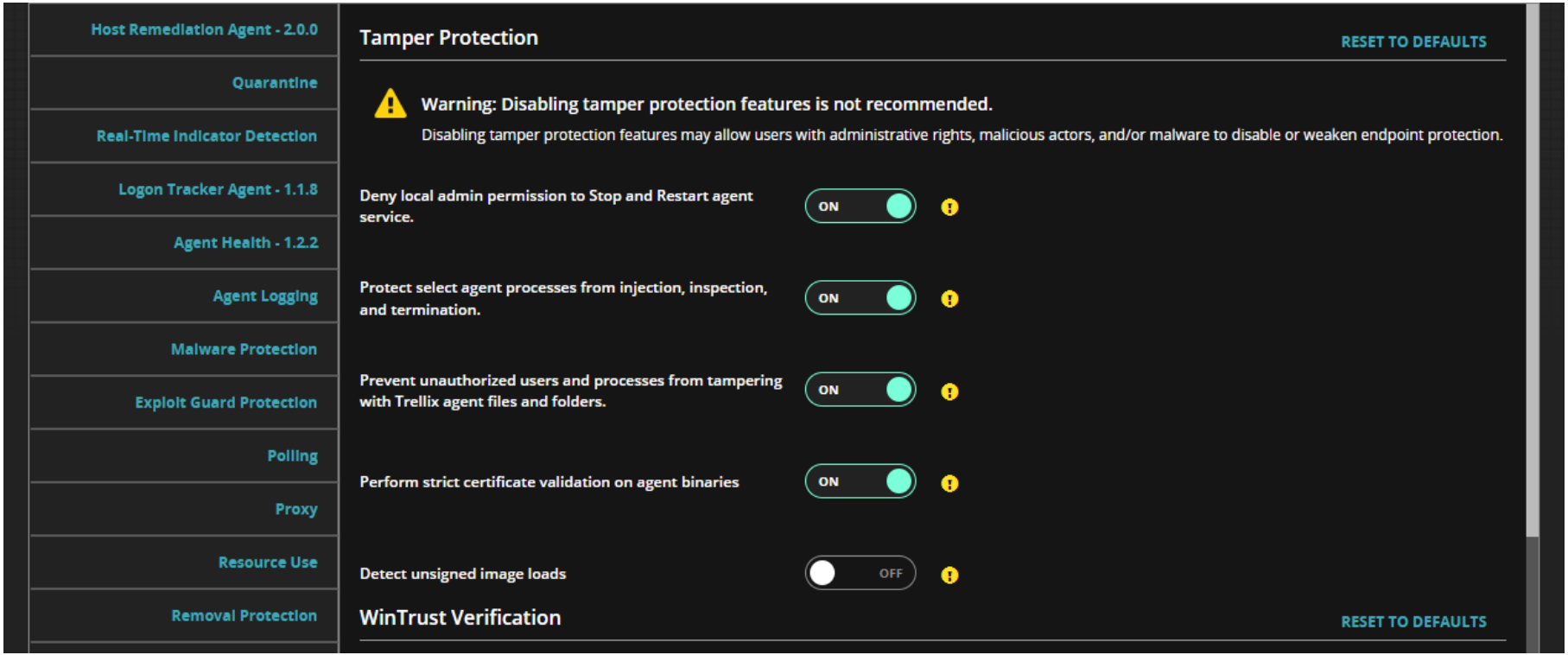
Trellix

Políticas: Removal Protection



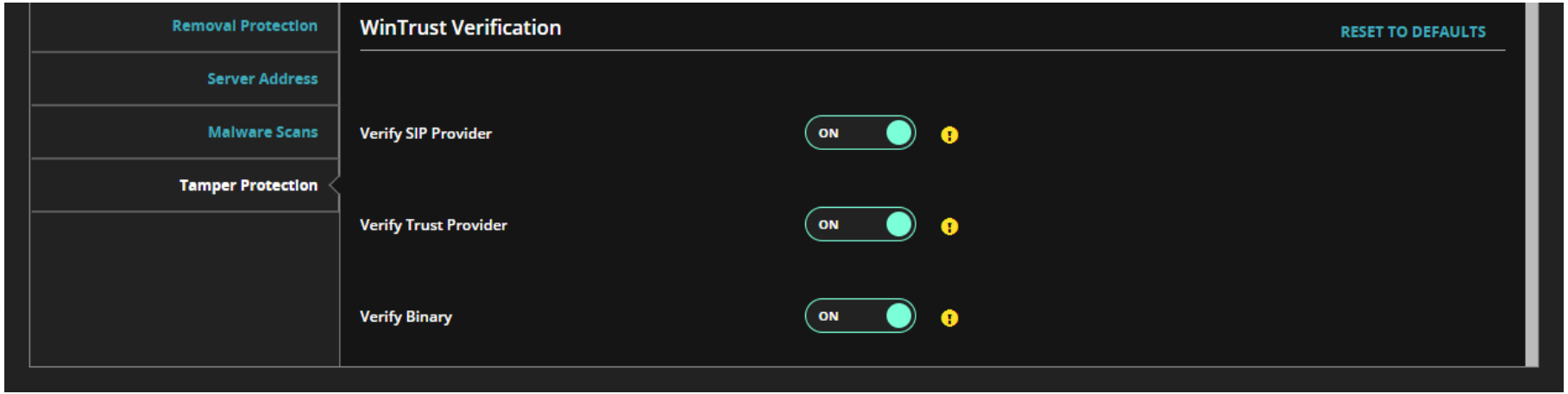
Trellix

Políticas: Tamper Protection



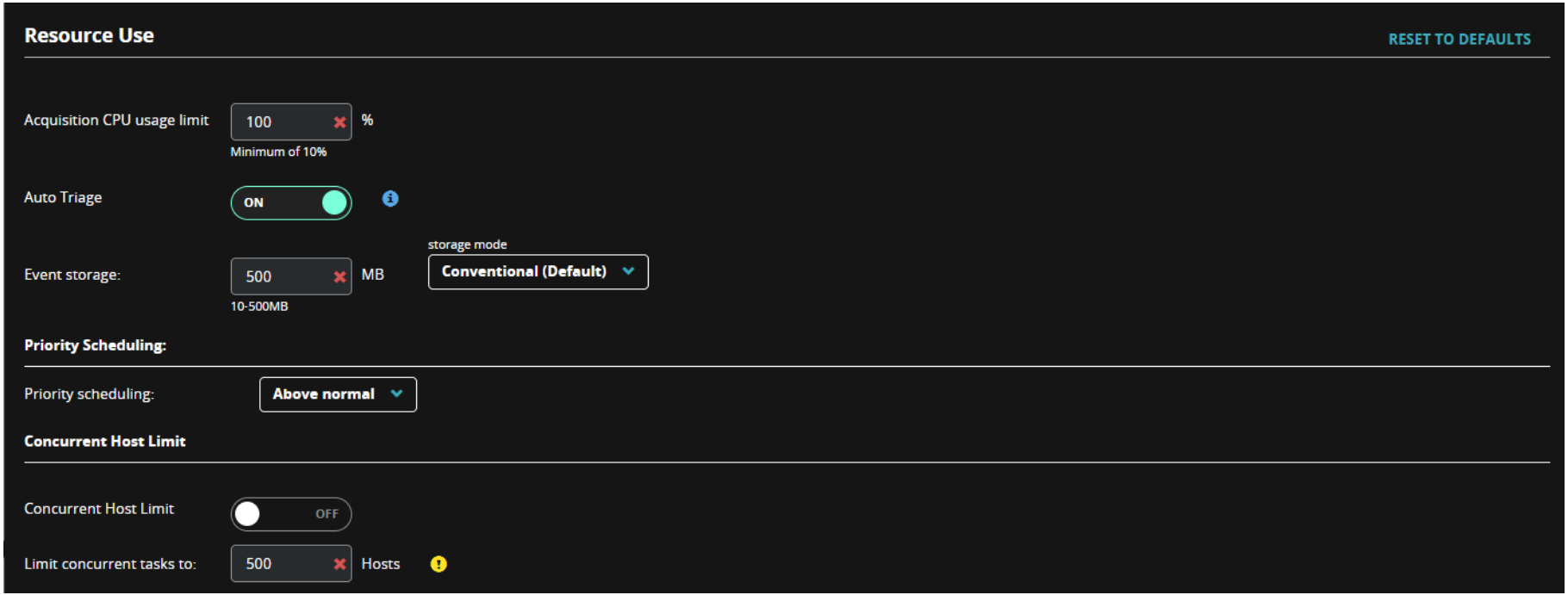
Trellix

Tamper Protection: Verificación WinTrust



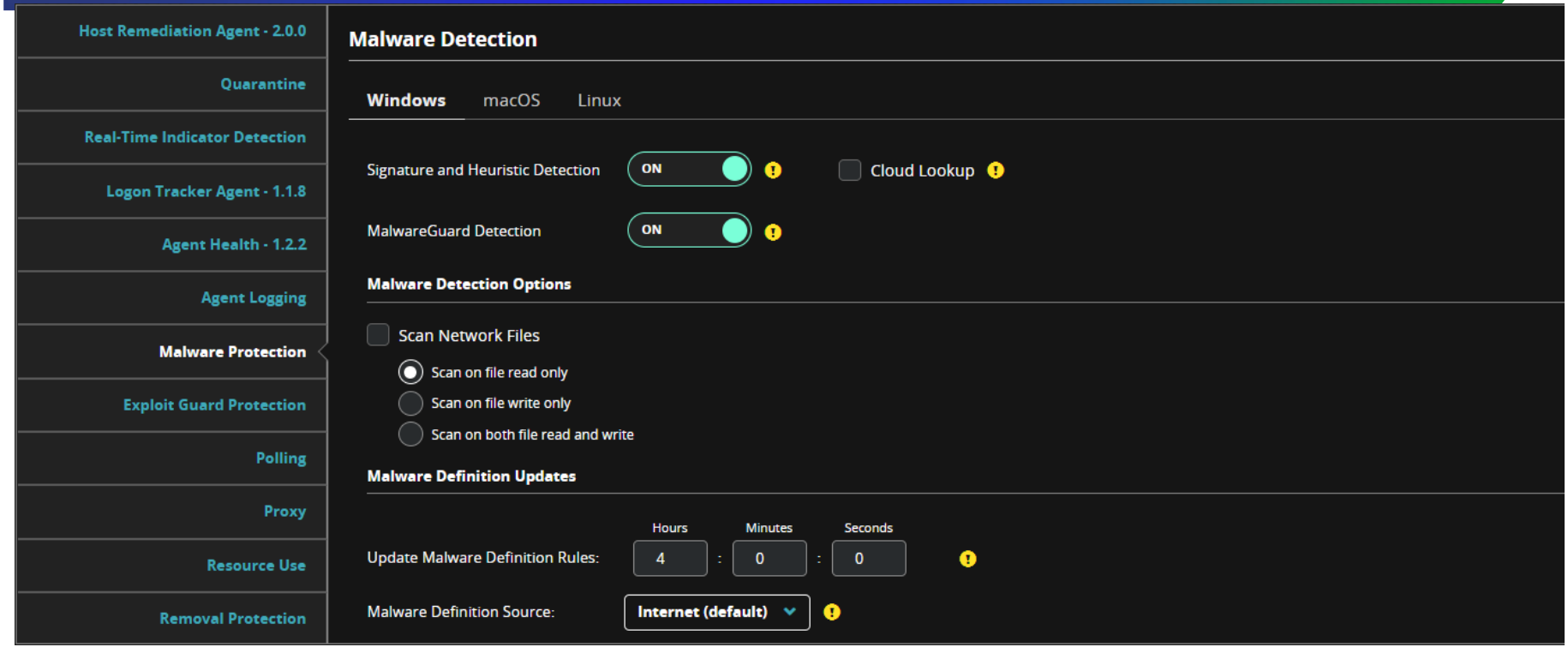
Trellix

Policies: Resource Use



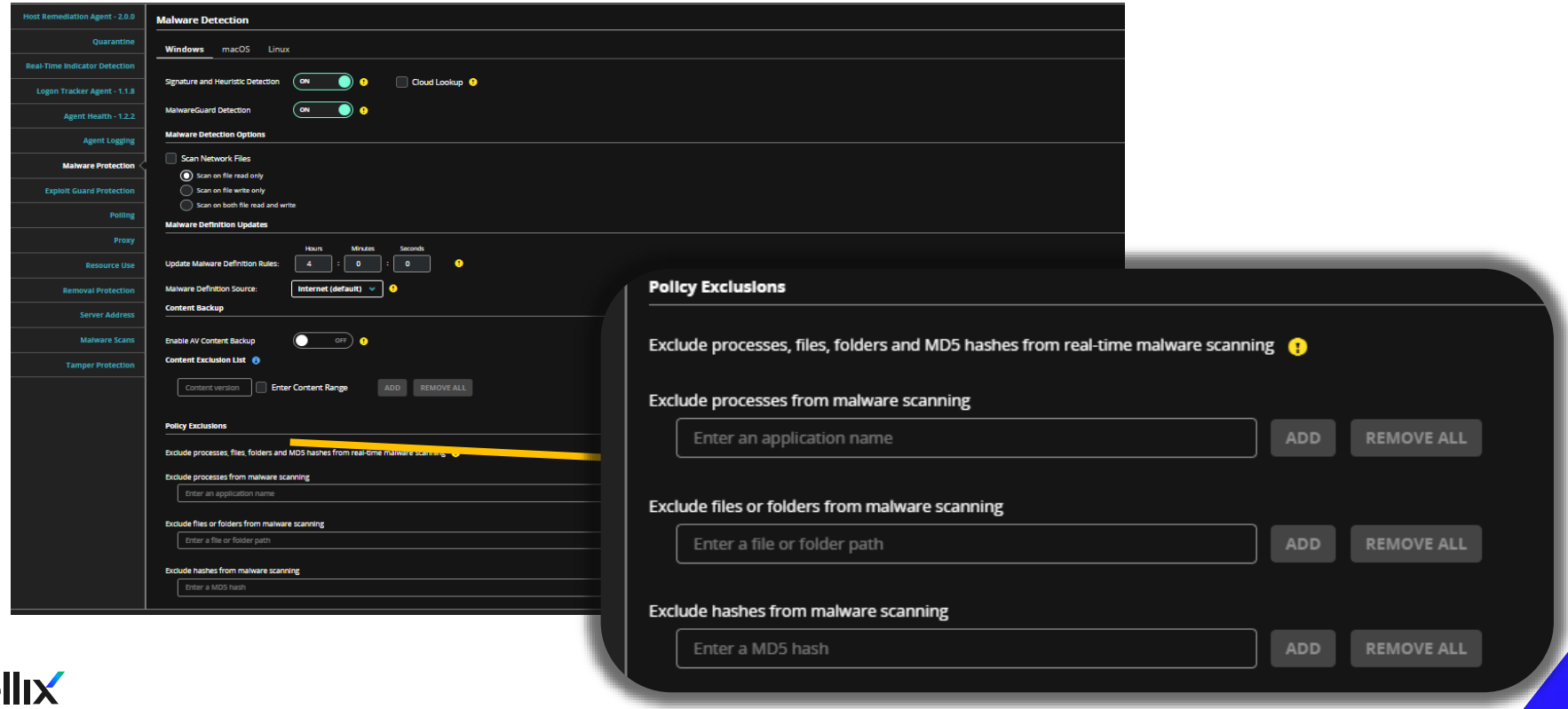
Trellix

Policies: Malware Protection



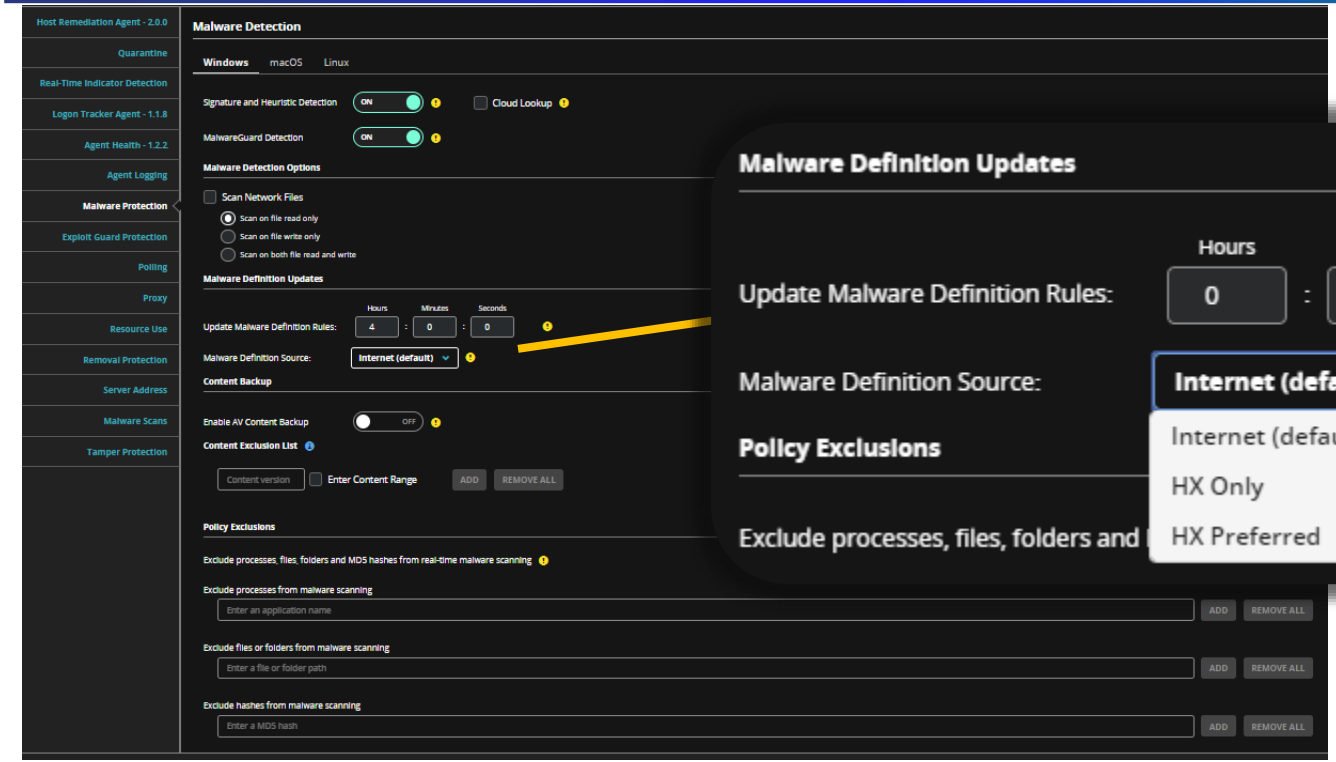
Trellix

Malware Protection: Policy Exclusions



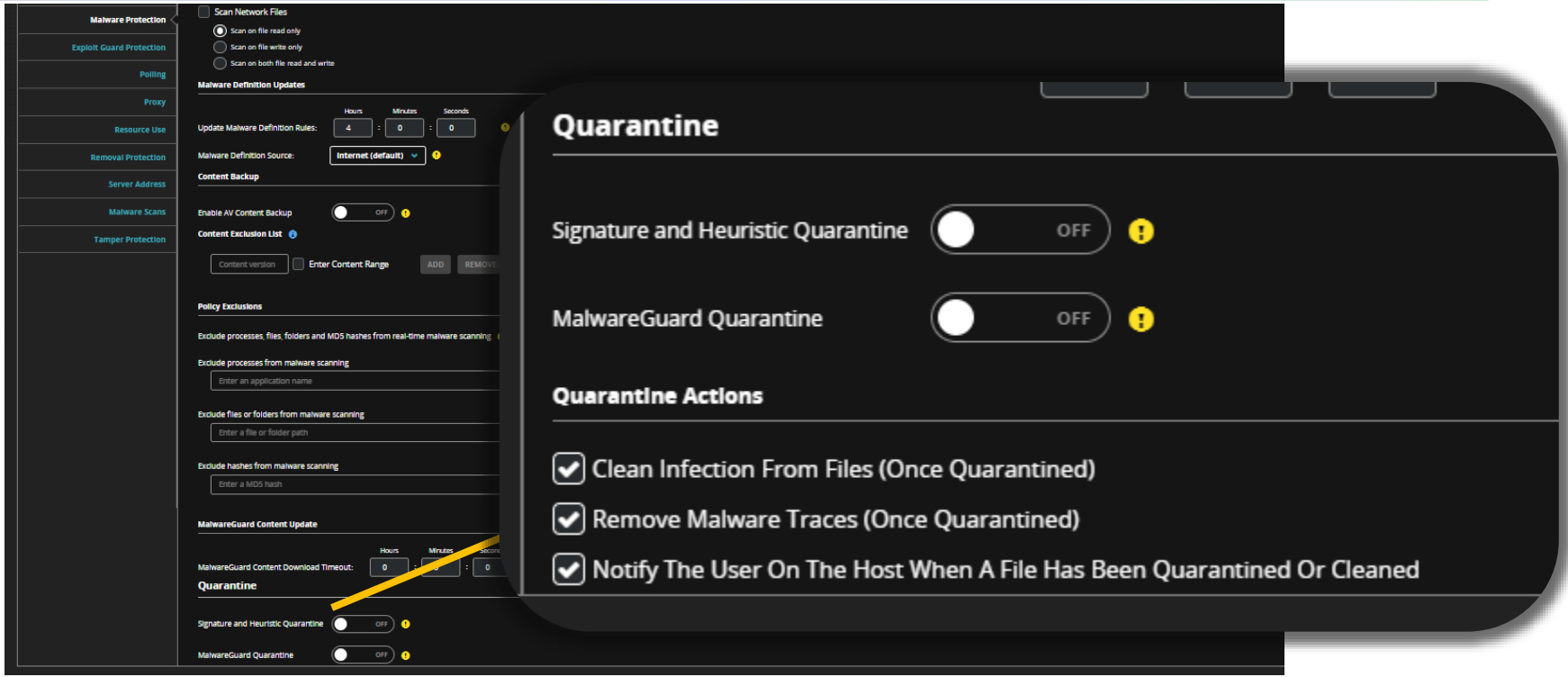
Trellix

Malware Protection: Definiciones



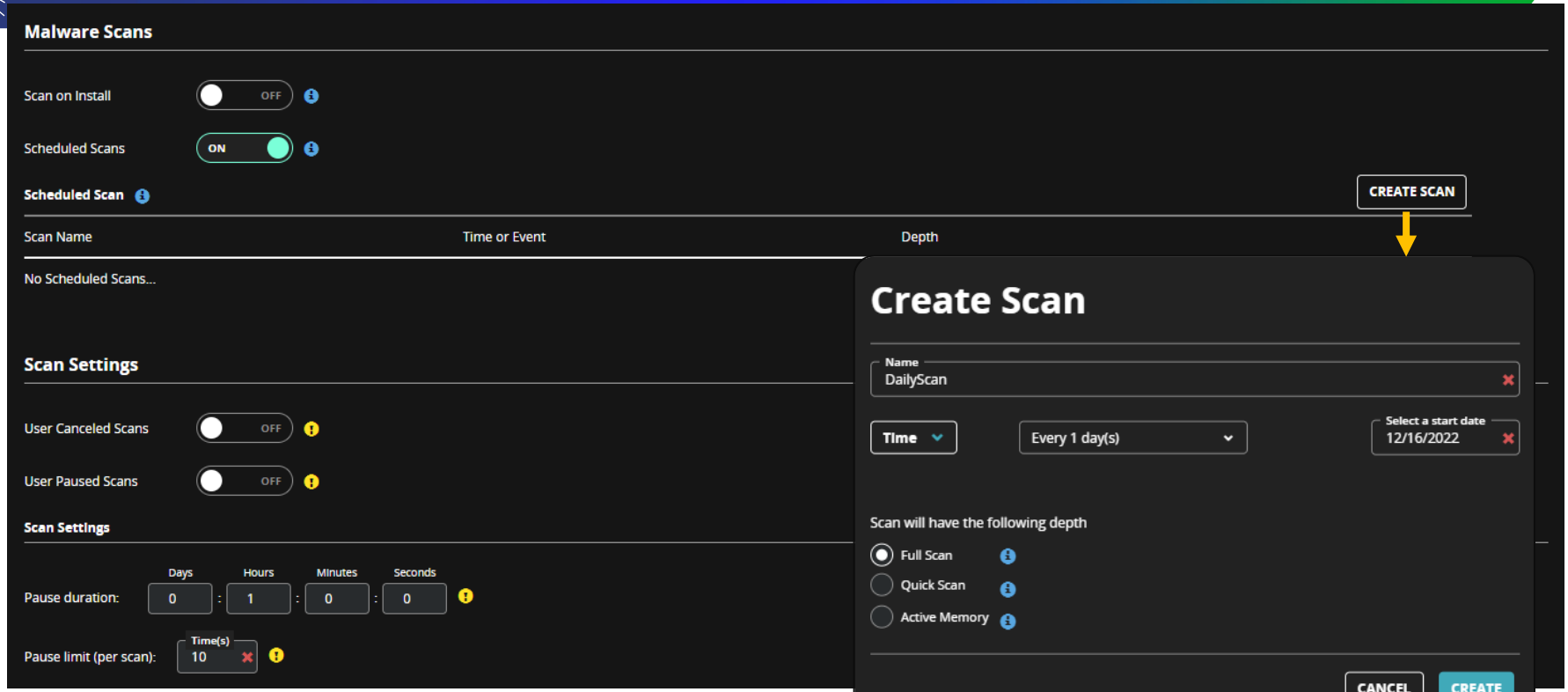
Trellix

Malware Protection: Quarantine



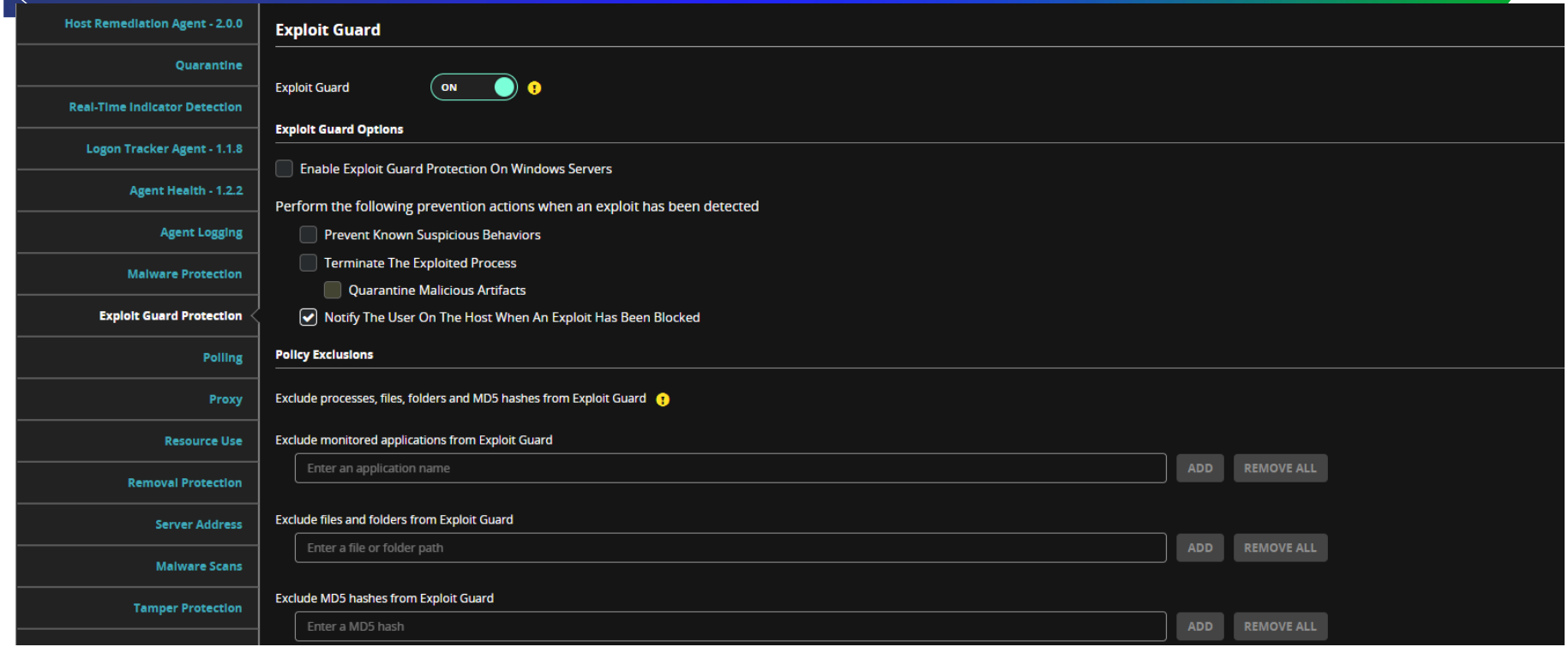
Trellix

Policies: Malware Scans



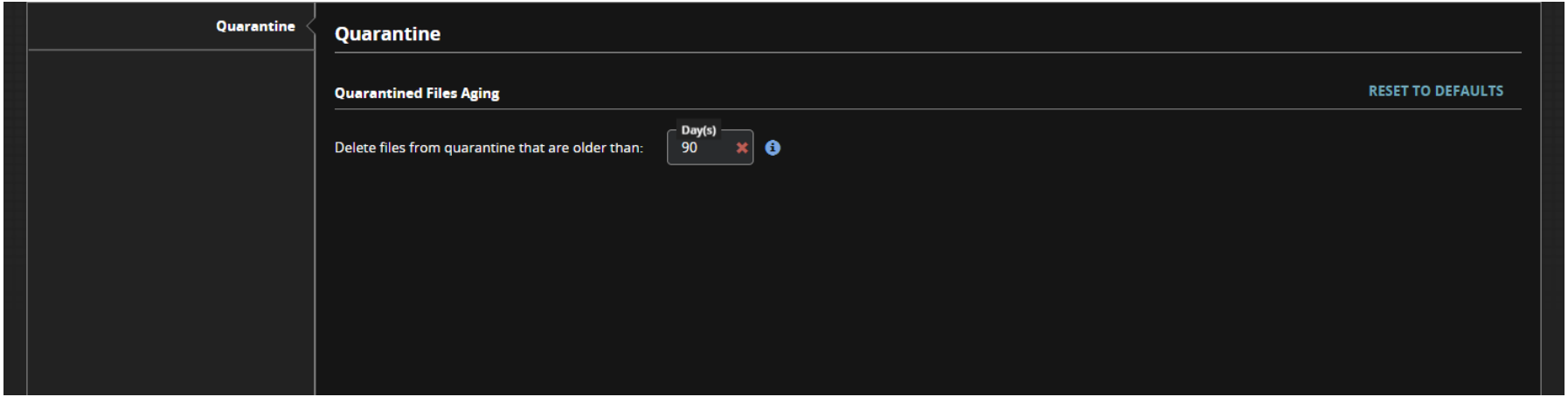
Trellix

Policies: Exploit Guard



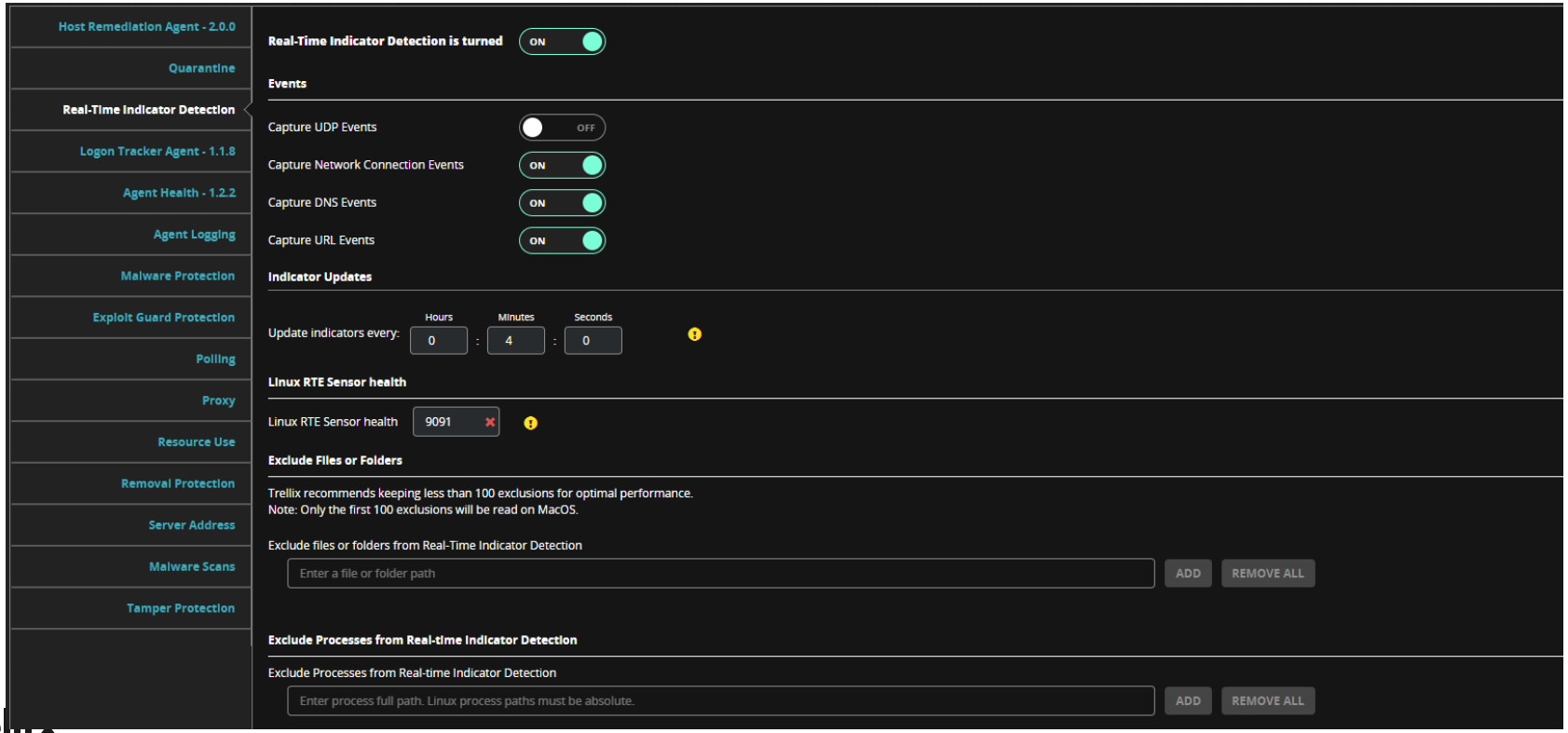
Trellix

Quarantine



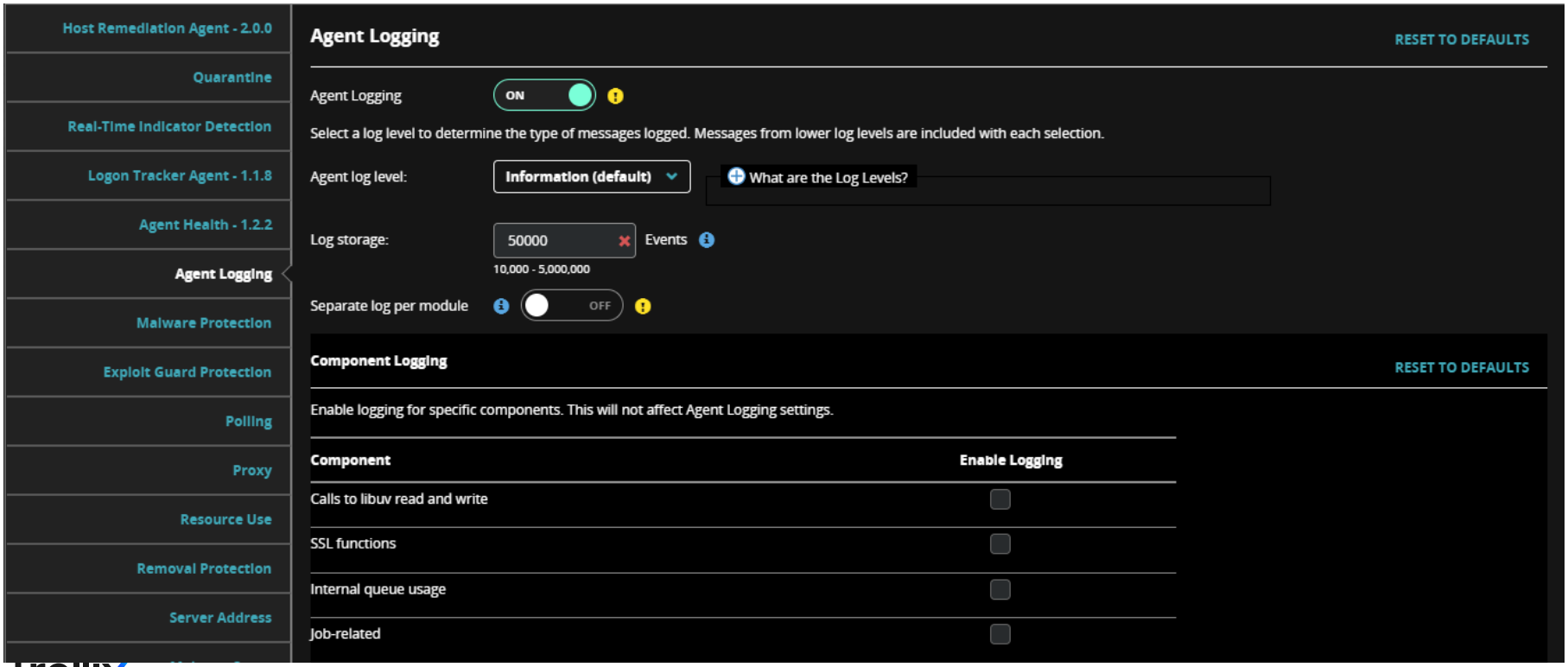
Trellix

Policies: Real-Time Indicator Detection (RTID)

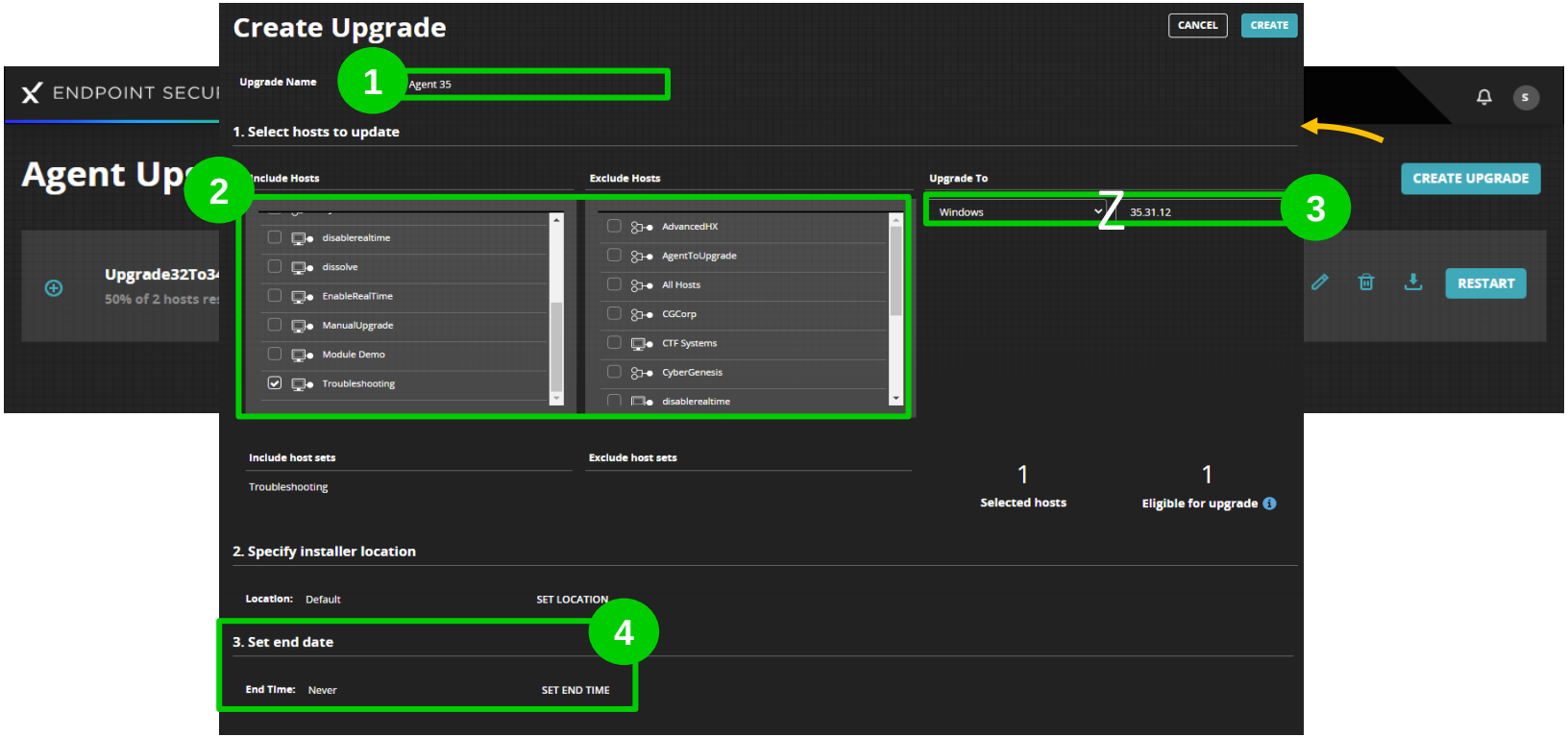


Trellix

Policies: Agent Logging



Policies: Agent Upgrades



Agent Management – Enterprise Installation

1

Priority	Policy Name	Status All	First Created	Last Modified	Actions
1	Agent Default policy	Enabled	5 days ago	5 days ago	Edit Policy

2

Version	Uploaded	Platform	
33.46.0	2021-05-28 16:48:32Z	Windows	DOWNLOAD AGENT INSTALLER
33.46.0	2021-05-28 16:48:27Z	Mac OS X	DOWNLOAD AGENT INSTALLER

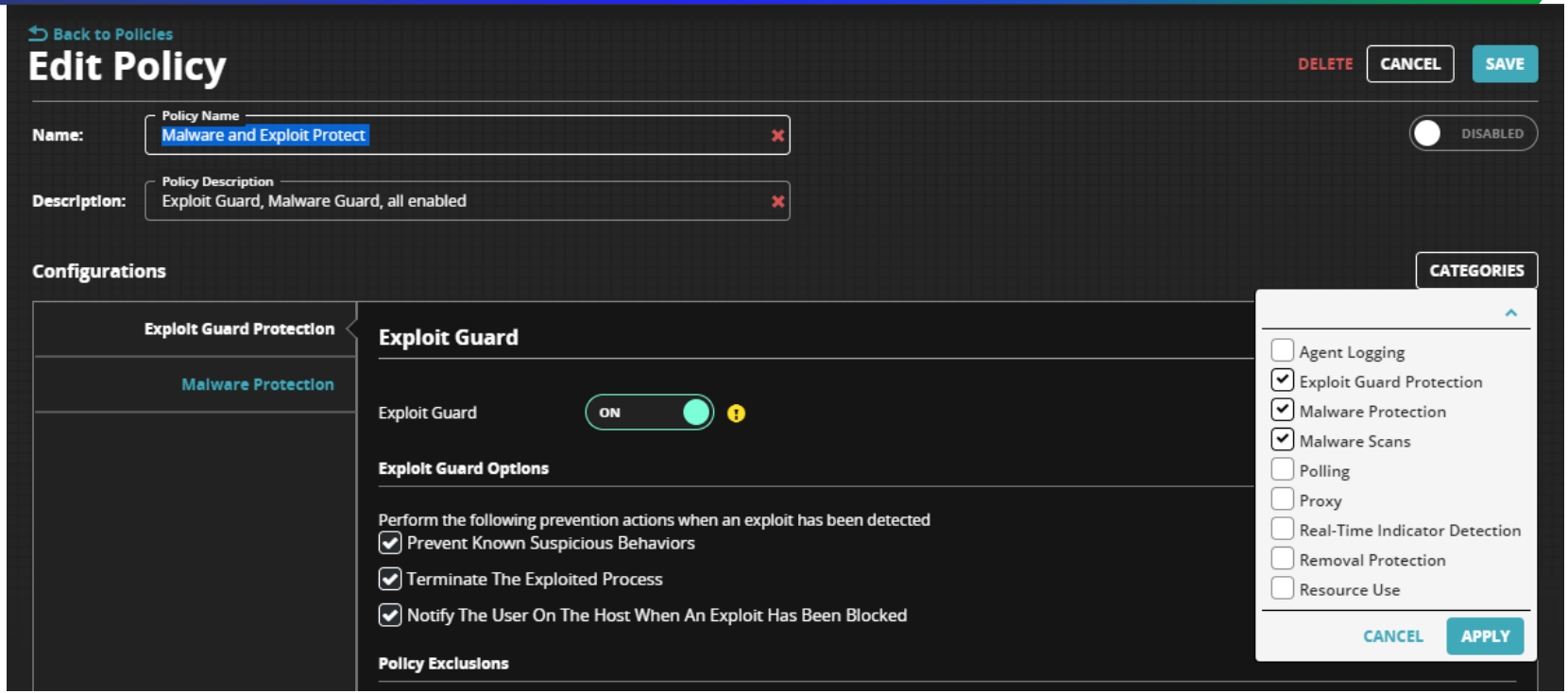
3

Test

4

Trellix

Custom Policies

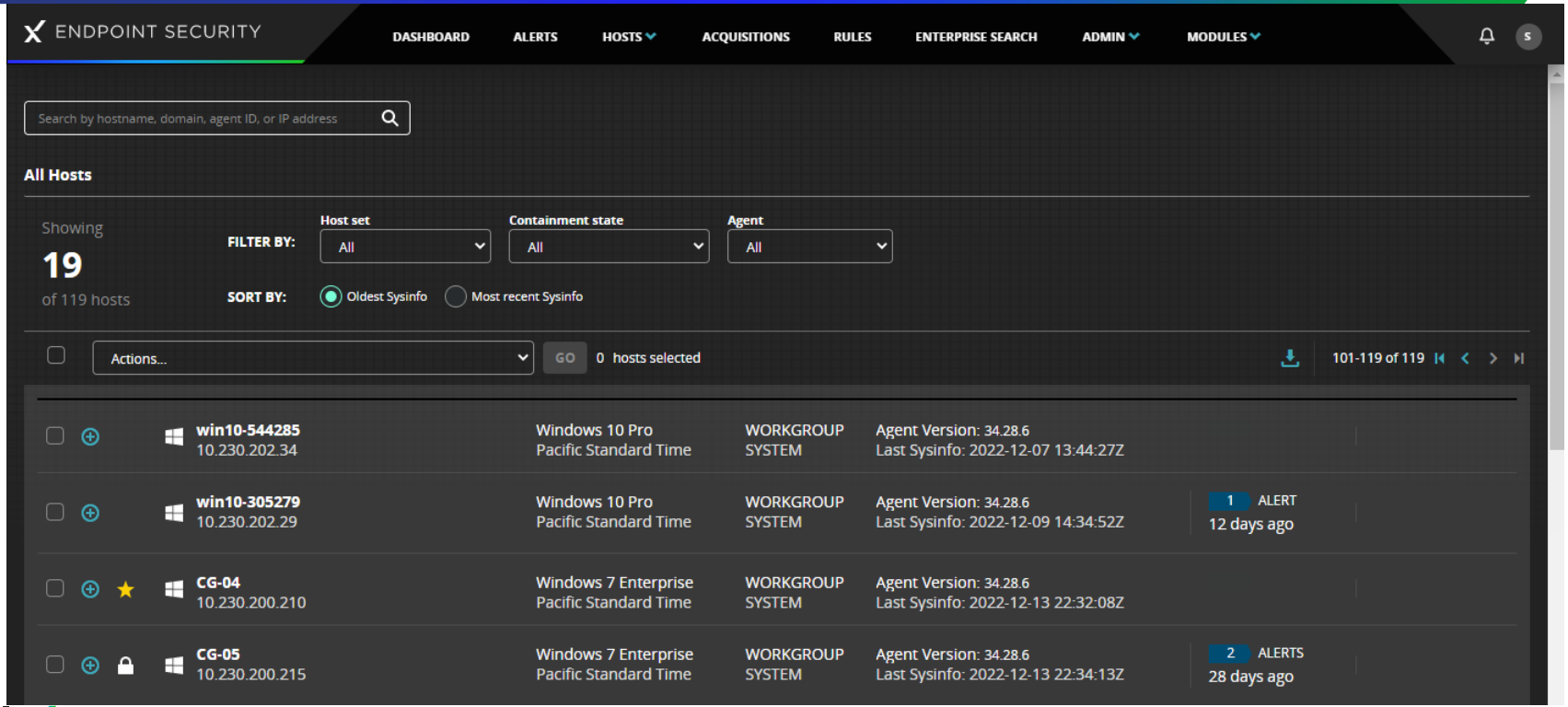


Trellix

Compatibilidad del agente

AGENT: V35						
Windows	**Audit**	**Real Time IOC**	**ExploitGuard**	**Malware Protection**	**MalwareGuard**	**IA Modules**
Windows 7	✓	✓	✓	✓	✓	✓
Windows 8, 8.1	✓	✓	✓	✓	✓	✓
Windows 10	✓	✓	✓	✓	✓	✓
Windows 11	✓	✓	✓	✓	✓	✓
Server 2008R2	✓	✓	✓	✓	✓	✓
Server 2012 & 2012R2	✓	✓	✓	✓	✓	✓
Server 2016	✓	✓	✓	✓	✓	✓
Server 2019	✓	✓	✓	✓	✓	✓
Server 2022	✓	✓	✓	✓	✓	✓
macOS	**Audit**	**Real Time IOC**	**ExploitGuard**	**Malware Protection**	**MalwareGuard**	**IA Modules**
macOS 11.0 – 11.6	✓	✓	X	✓	X	✓
macOS 12.0 – 12.6	✓	✓	X	✓	X	✓
macOS 13.0	✓	✓	X	✓	X	✓
Linux	**Audit**	**Real Time IOC**	**ExploitGuard**	**Malware Protection**	**MalwareGuard**	**IA Modules**
RHEL 6.10, 7.2-7.9, 8.0-8.6	✓	✓	X	✓	X	✓
CentOS 6.10, 7.2-7.9, 8.0 - 8.5	✓	✓	X	✓	X	✓
Rocky Linux 8.4 – 8.5	✓	✓	X	✓	X	✓
Ubuntu 14.04, 16.04, 18.0.4, 19.04, 20.04, 22.04	✓	✓	X	✓	X	✓
SUSE Enterprise Linux Server 12 SP4-SP5, 15 GA, SP1 - SP3	✓	✓	X	✓	X	✓
OpenSUSE Leap 15.1, 15.2, 15.3	✓	✓	X	✓	X	✓
Amazon AMI 2018.3, Amazon Linux 2	✓	✓	X	✓	X	✓
Oracle Linux 6.10, 7.7 -7.9, 8.0 - 8.6	✓	✓	X	✓	X	✓

Host Management



Trellix

Host Details

server-db
10.230.203.203

Windows Server 2019 Sta...
Central Standard Time

CYBERGENESIS
SYSTEM

Agent Version: 34.28.6
Last Sysinfo: 2022-08-12 23:11:25Z

IP Address	10.230.203.203 fe80::84c3:edc8:b8e1:85ca 127.0.0.1 ::1
Client IP	10.230.203.203
Agent ID	xHdOFxo3vUkb7RbKsHq1AP
Agent Version	34.28.6
OS	Windows Server 2019 Standard
Patch	....
Kernel	....
KernelServices Status	Loaded
Bit Level	64-bit
Domain	CYBERGENESIS
Active Directory: Domain Components	cybergenesis, local?
Active Directory: Organizational Units	
Active Directory: Common Names	Computers, SERVER-DB
Timezone	Central Standard Time
GMT Offset	UTC-6:00

USER

Primary User	SYSTEM
Registered Org	Organization
Registered Owner	Owner

NETWORK ADAPTERS

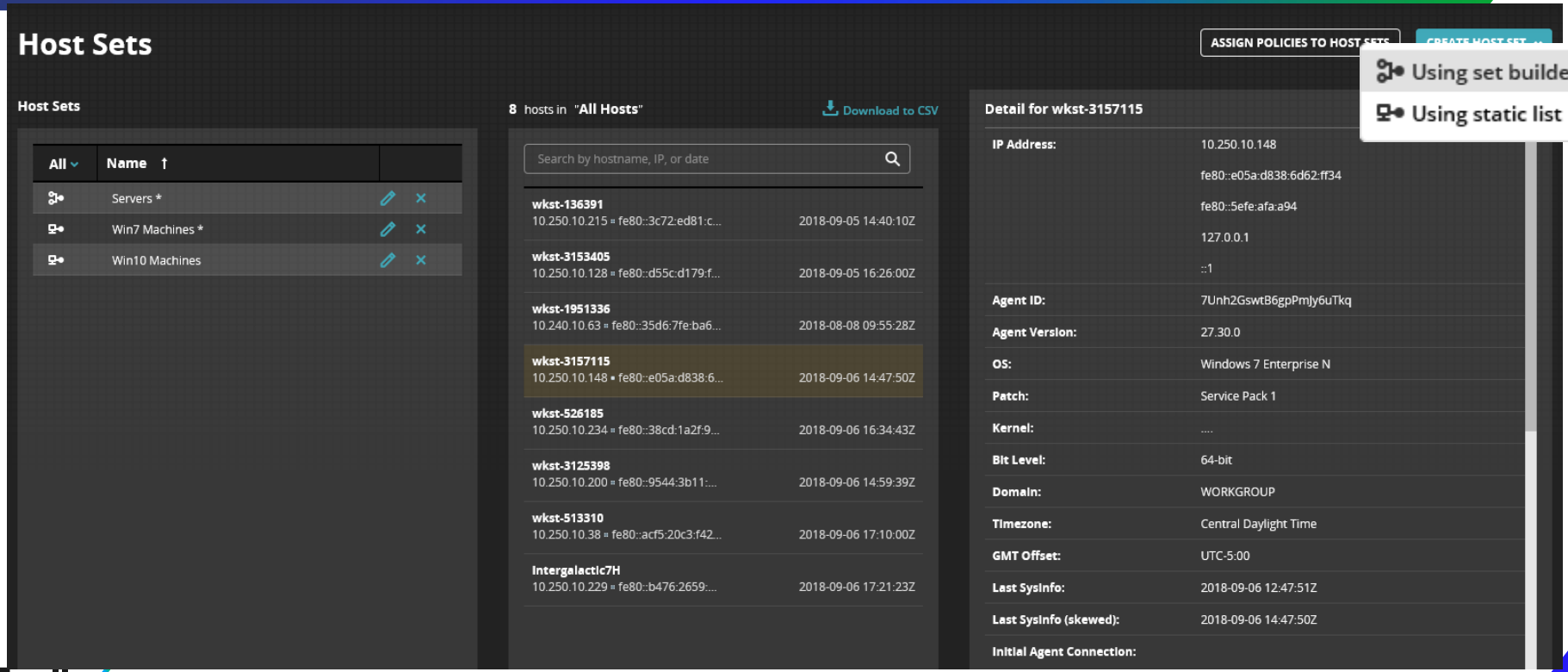
Red Hat VirtIO Ethernet Adapter

Subnet Mask	255.255.252.0
IP Address	10.230.203.203 fe80::84c3:edc8:b8e1:85ca
Name	{3A4C7C24-D7B0-4462-8F23-F386D4128247}
MAC	ea-80-dc-90-91-e9
DHCP Address	....
IP Gateway Address	10.230.203.254
Lease Obtained Date	....
Lease Expiry Date	....

Software Loopback Interface 1

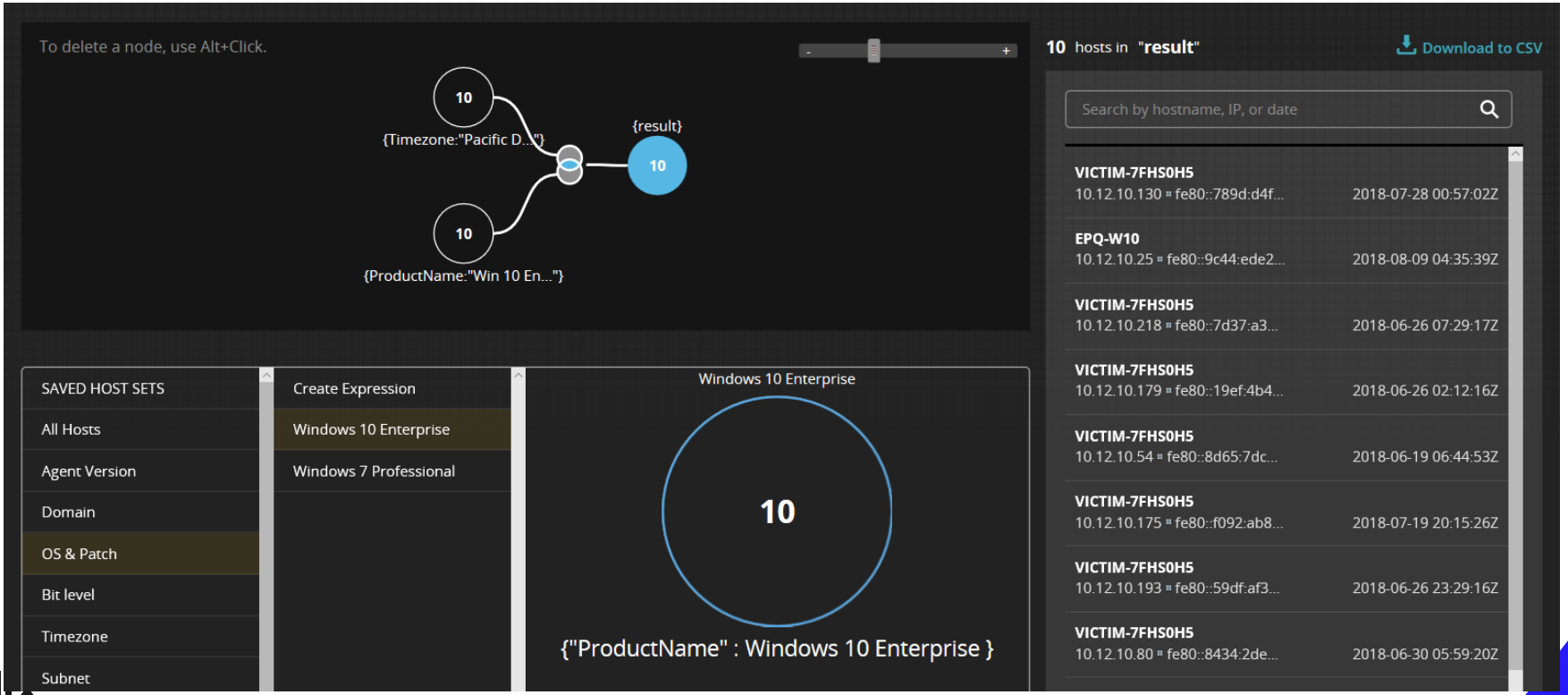
Subnet Mask	....

Host Sets



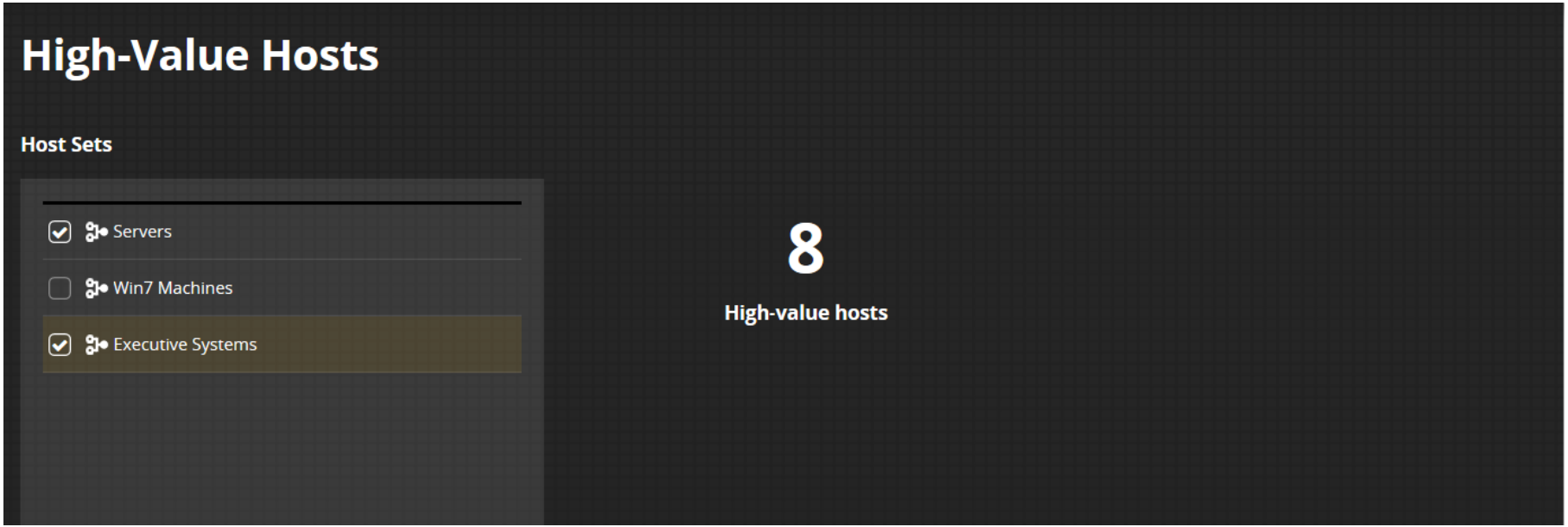
Trellix

Standard Host Sets (Grupos dinámicos)



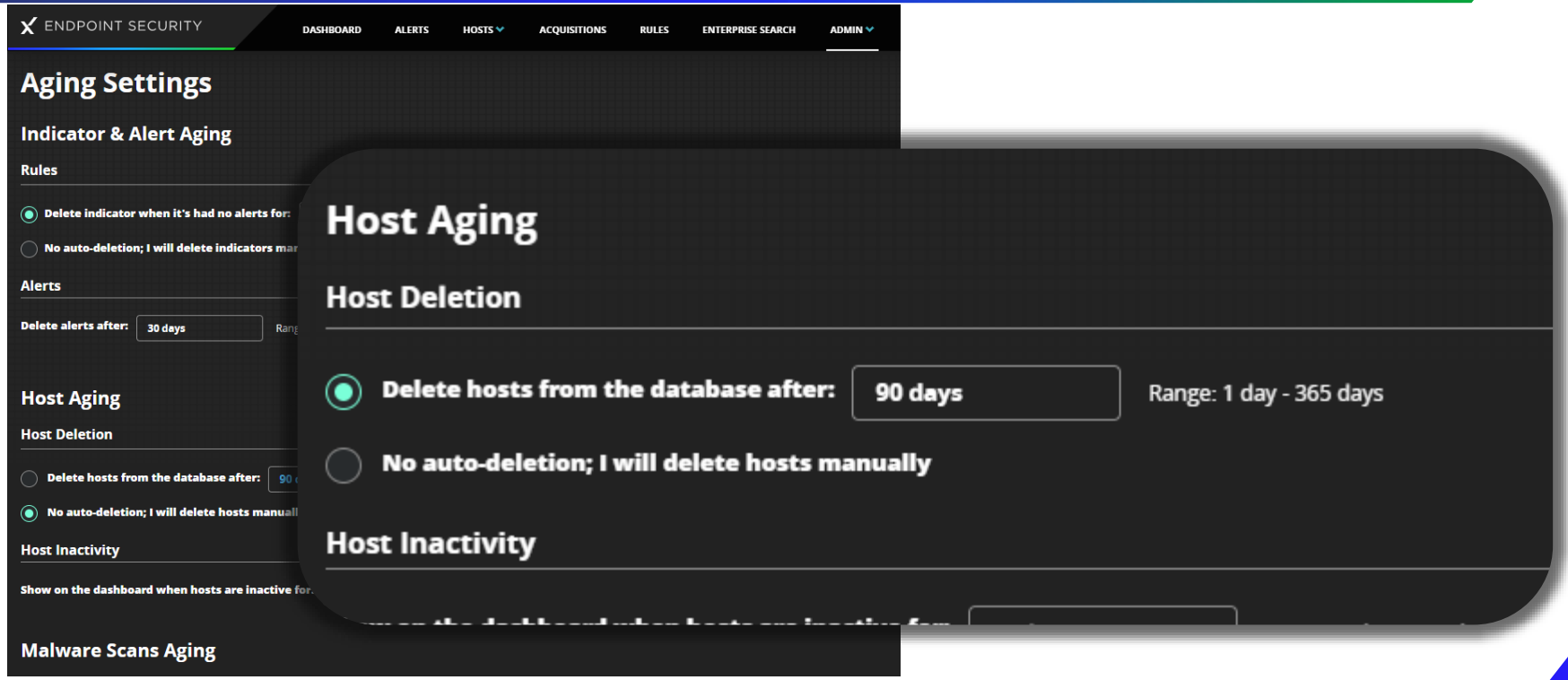
Trellix

High Value Hosts



Trellix

Host Aging



Trellix

Resumen

Endpoint Security Operational Overview

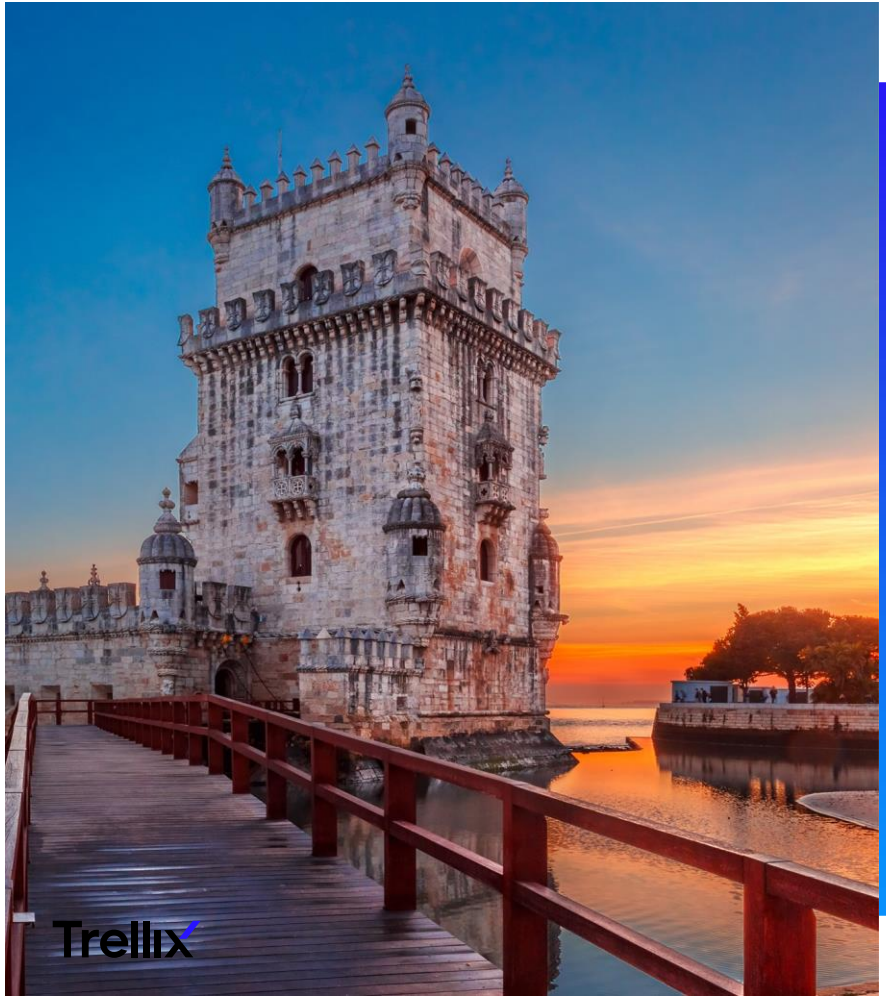
Product features

- User Interfaces
- Trellix Endpoint Security agent
- Ring buffer

Deployments

- Appliance configuration
- Agent management and configuration
- Host management

Trellix



Agenda

Endpoint Security

Endpoint Security Alerts

- Reglas
- Tipos de alerta
- Resumen de triage

Identificar IOCs

- Enterprise Search
- File Acquisitions

Engines de detección

Exploit Guard

- Monitors commonly exploited applications
- Detection with option to block
- Trellix-managed detection

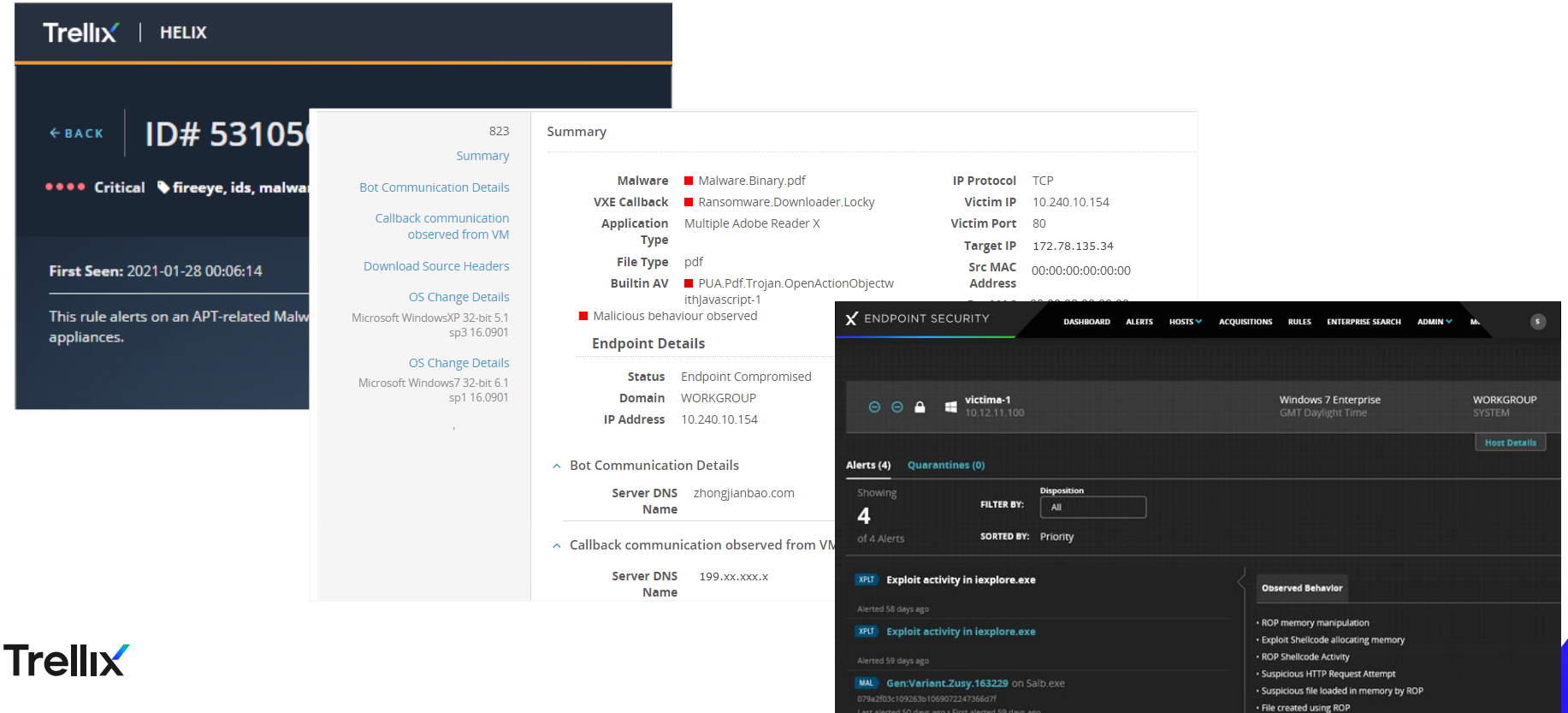
Malware Protection

- Signature-based
- Full AV Replacement
- Can configure quarantine
- Can configure Malware Scans
- MalwareGuard Machine Learning

Real-time Detection

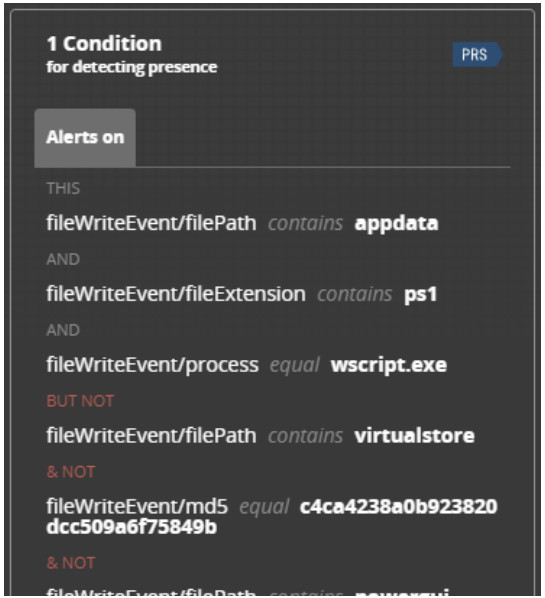
- Based on Agent events
- Trellix-provided and custom

Iniciar una investigación a partir de una alerta



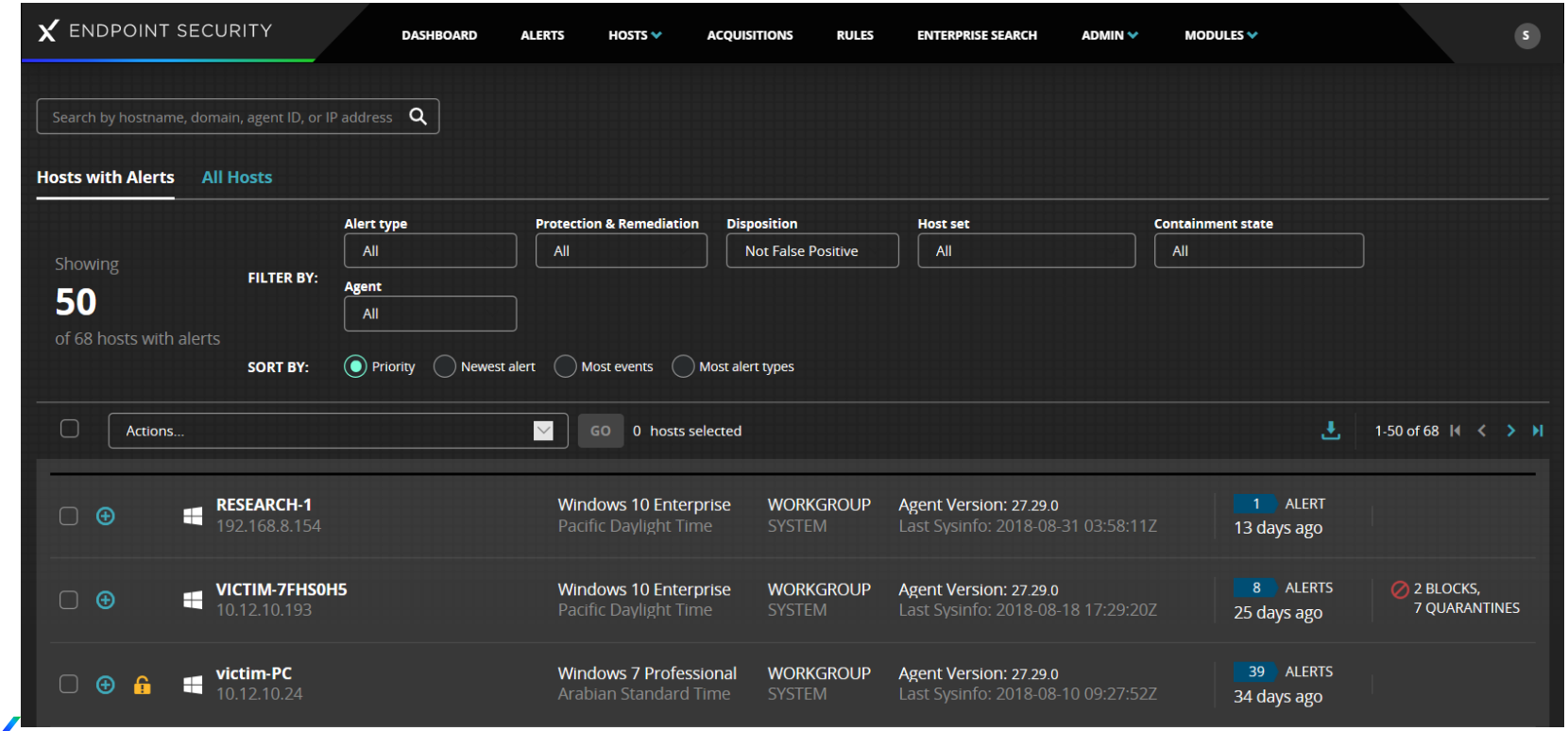
Trellix

Condiciones y tipos de indicadores



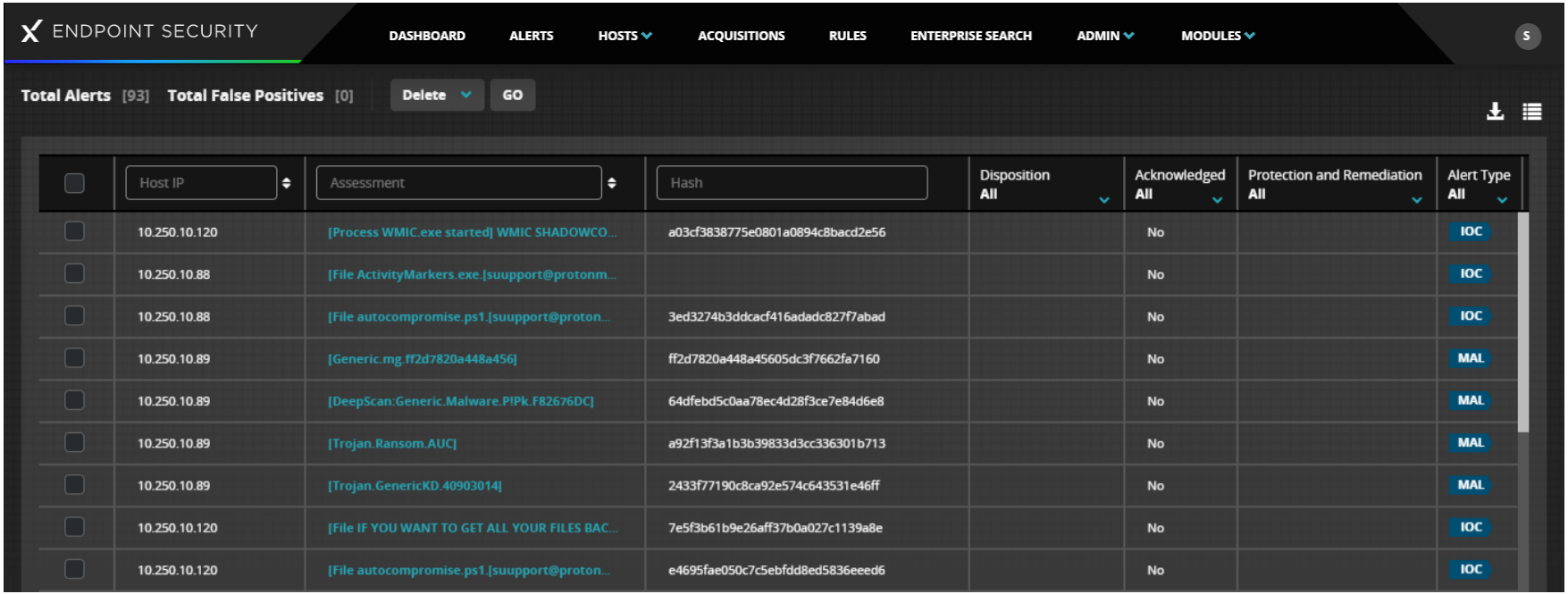
Trellix

Hosts con Alertas



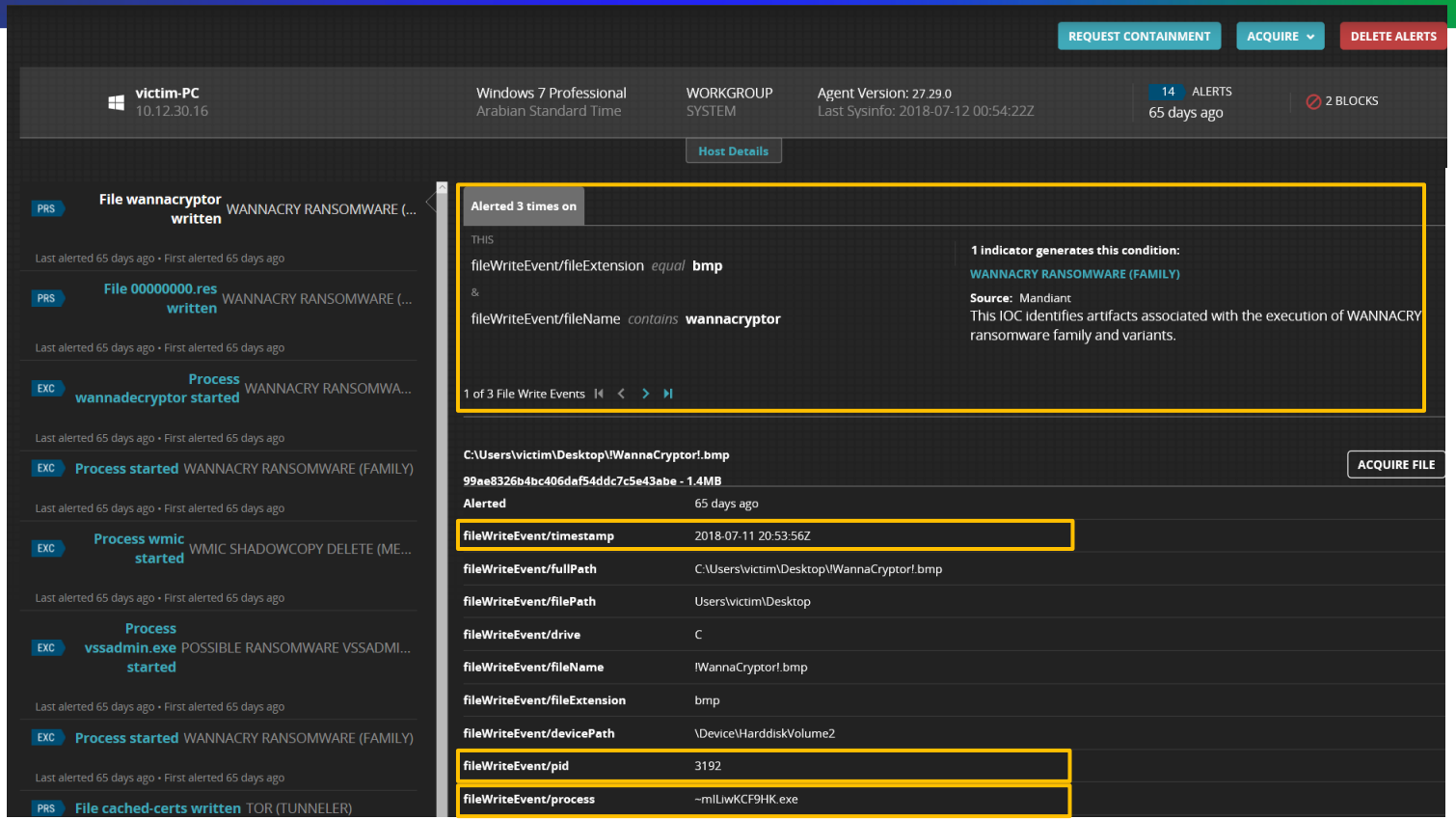
Trellix

Gestión de alertas

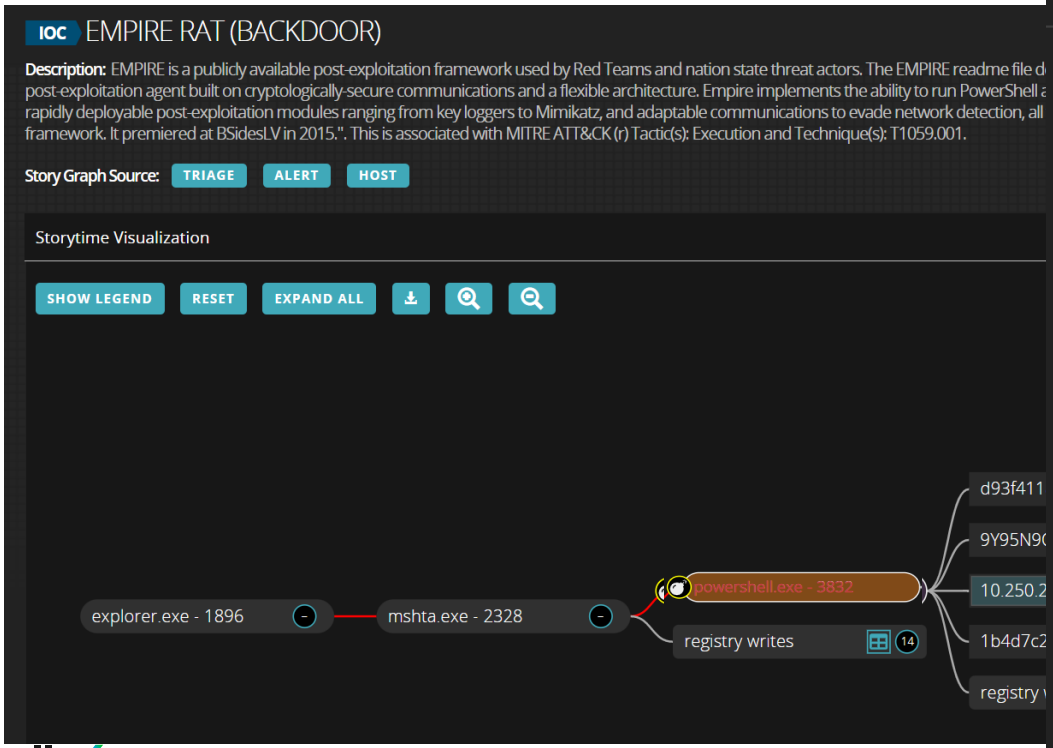


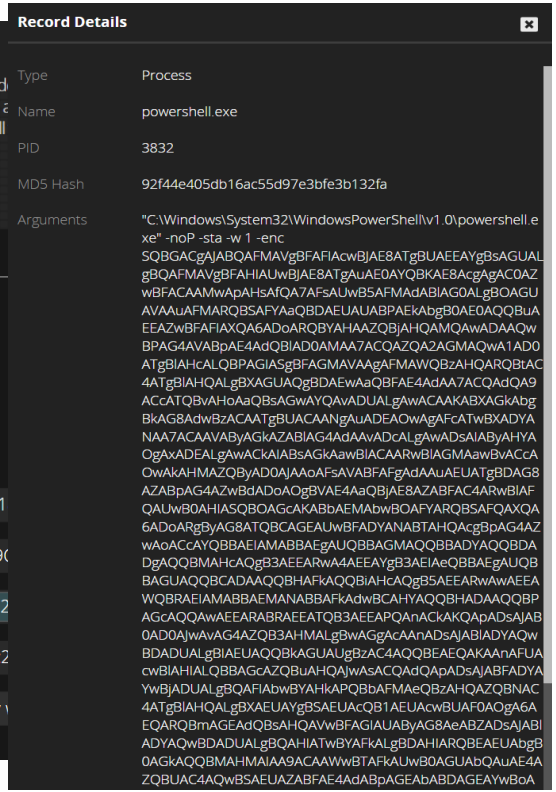
Trellix

Detalle de la alerta



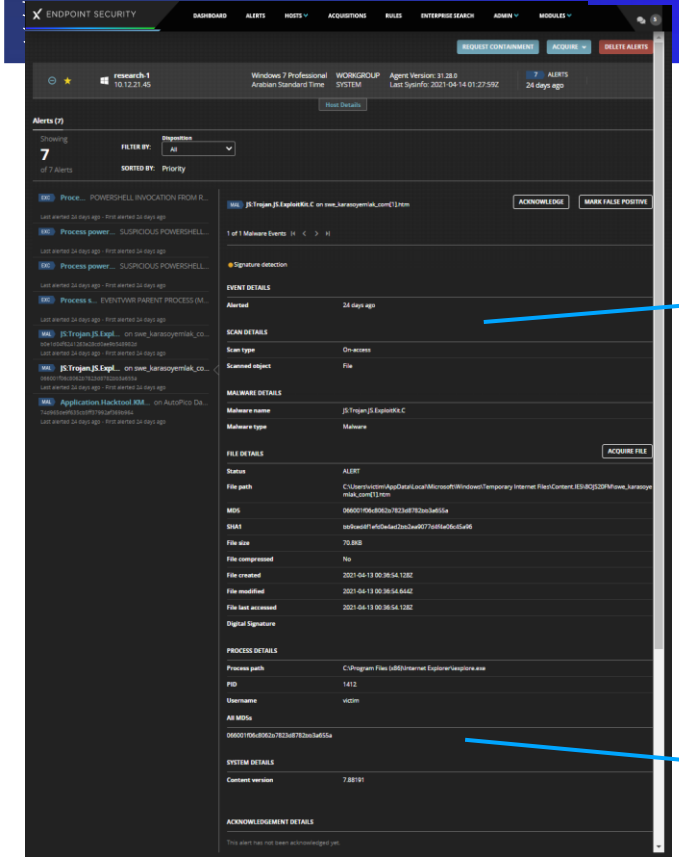
Línea de tiempo





Trellix

Caso de estudio



MAL **JS:Trojan.JS.ExploitKit.C** on swe_karasoyemlak_com[1].htm

1 of 1 Malware Events

Signature detection

EVENT DETAILS

Alerted	24 days ago

SCAN DETAILS

Scan type	On-access
Scanned object	File

MALWARE DETAILS

Malware name	JS:Trojan.JS.ExploitKit.C
Malware type	Malware

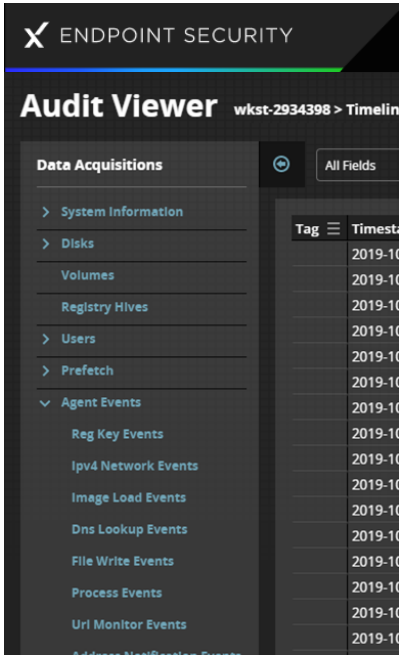
PROCESS DETAILS

Process path	C:\Program Files (x86)\Internet Explorer\iexplore.exe
PID	1412
Username	victim

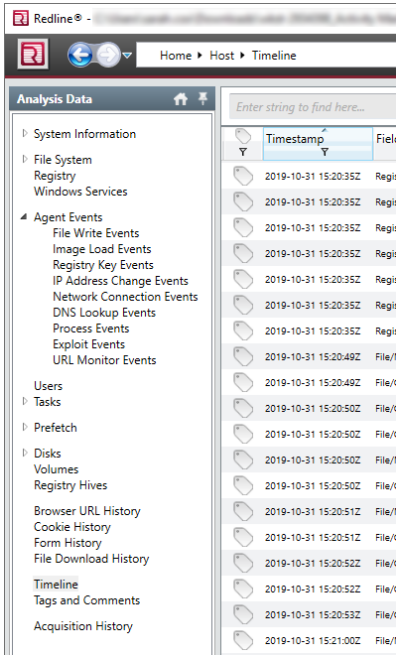
Opciones de análisis

Triage Summary

Audit Viewer

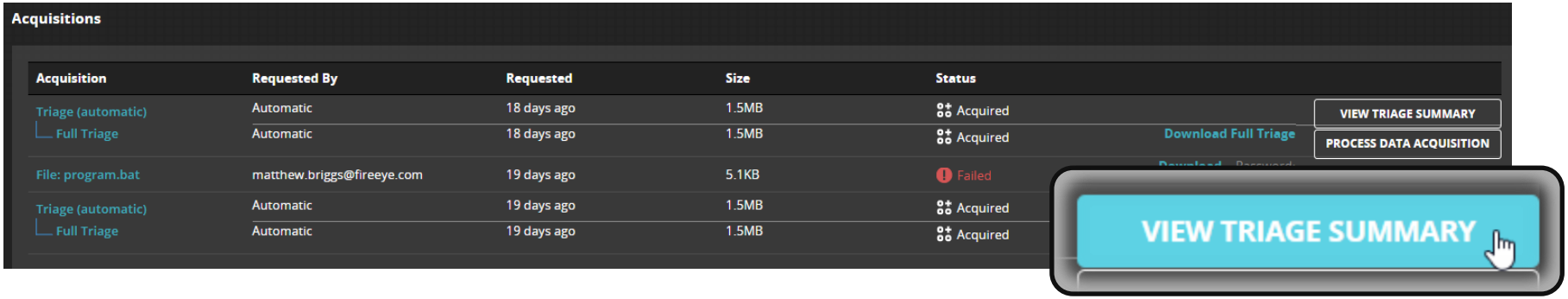


Redline



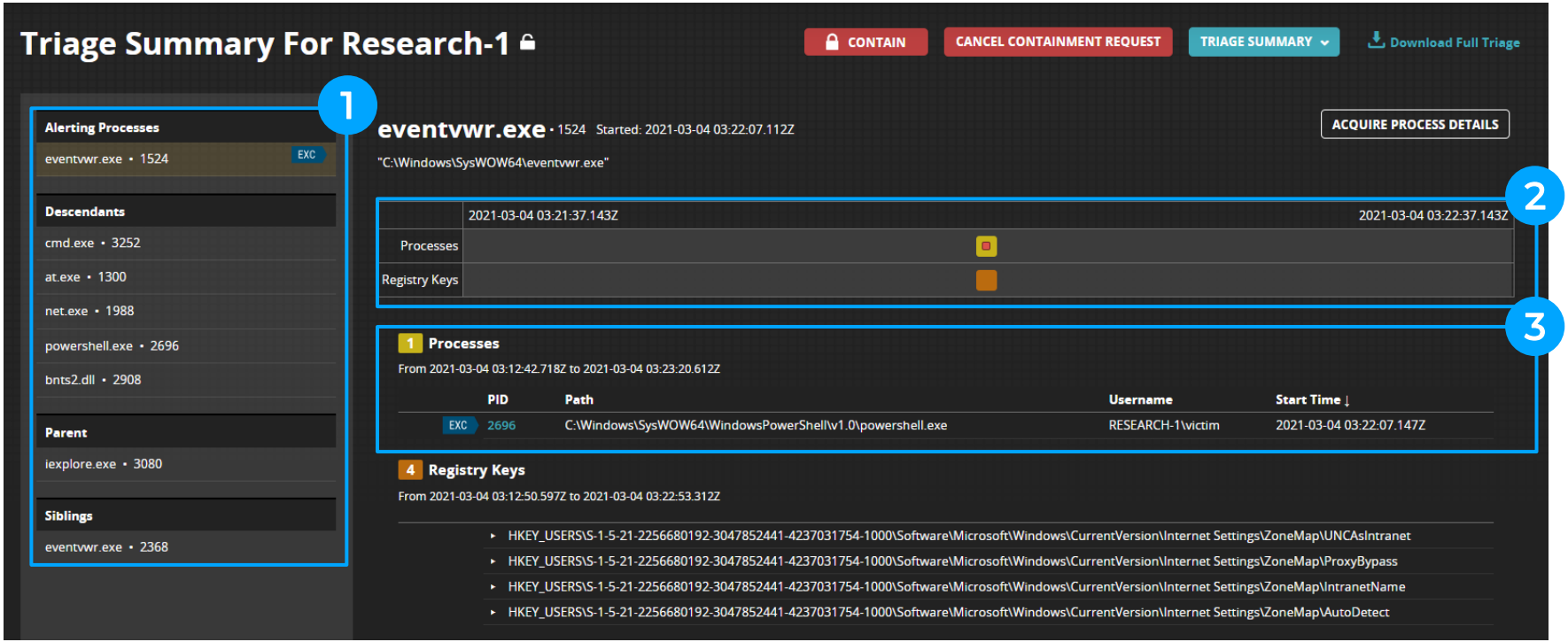
Trellix

Acceso al resumen del triage



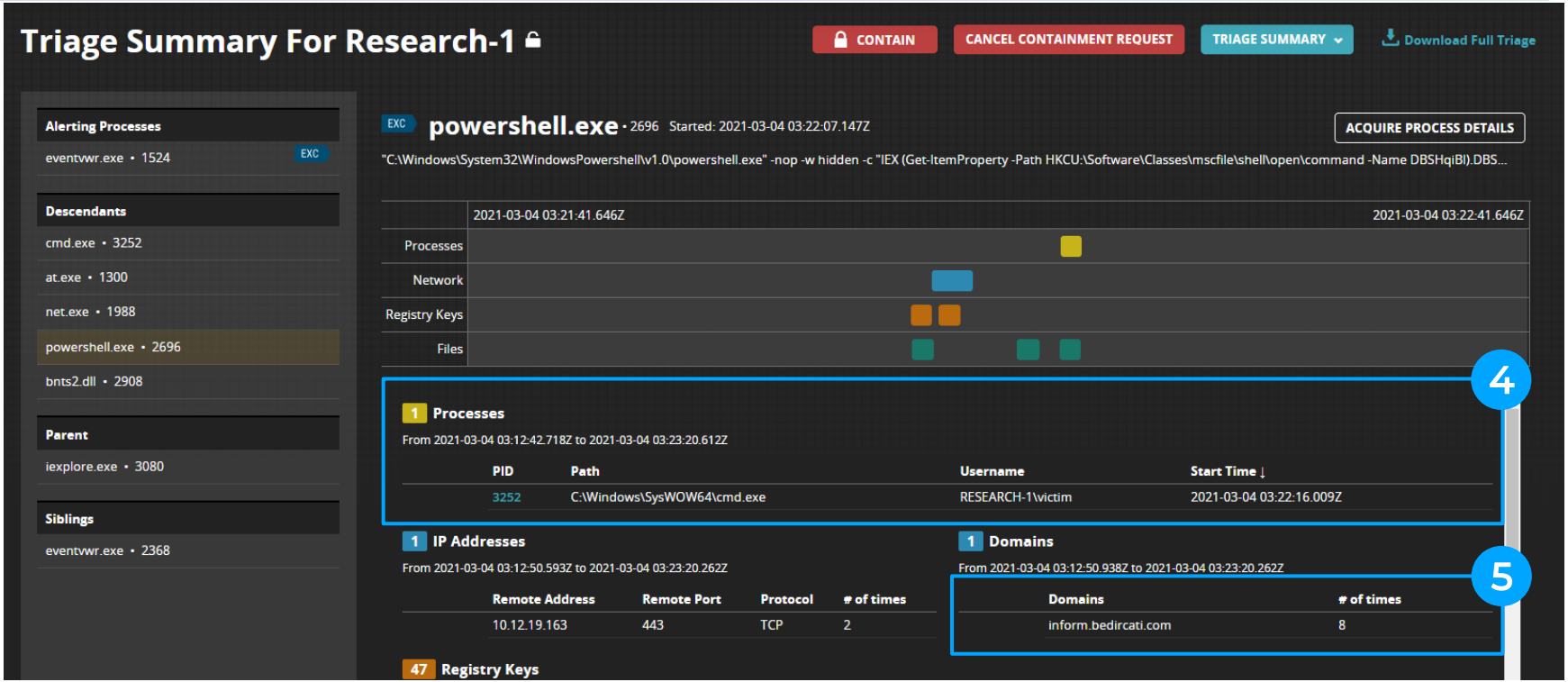
Trellix

Resumen del Triage



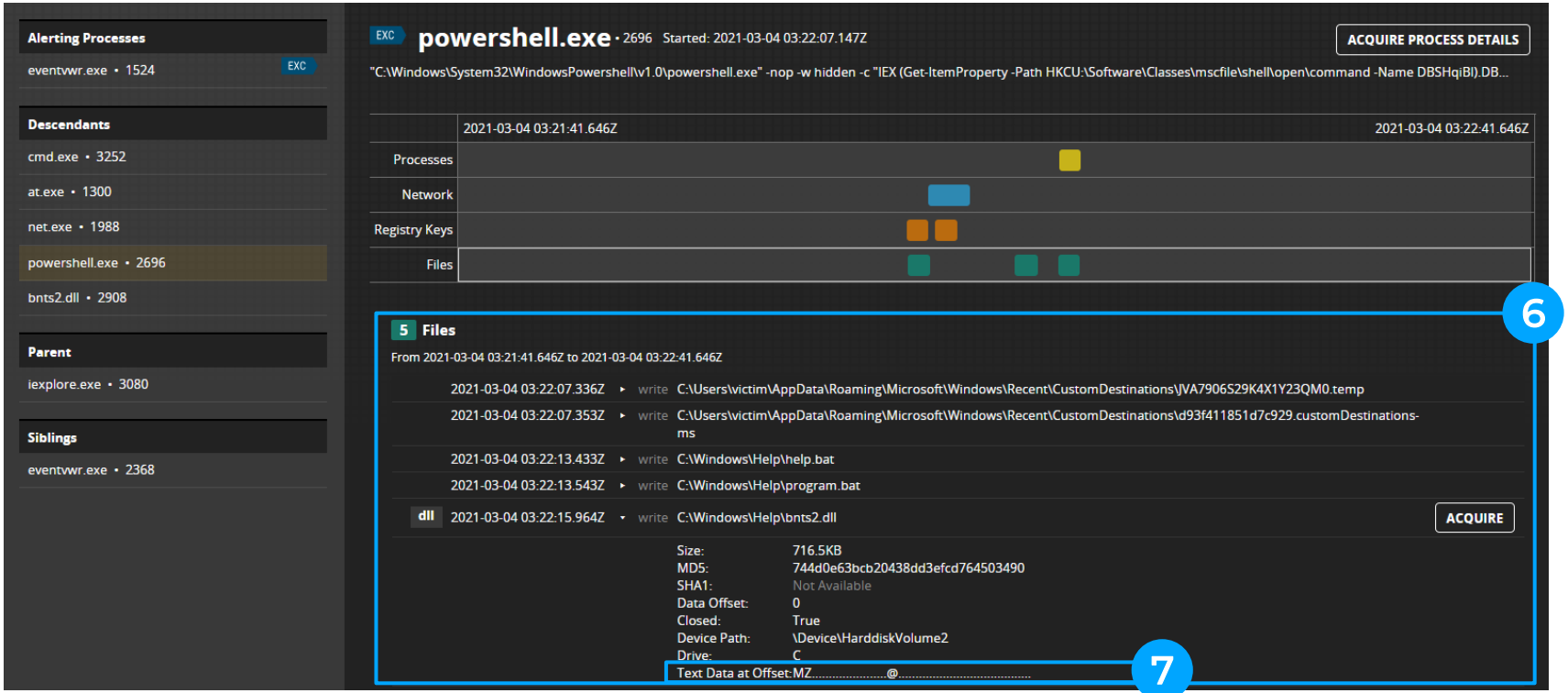
Trellix

Resumen del Triage – Procesos secundarios



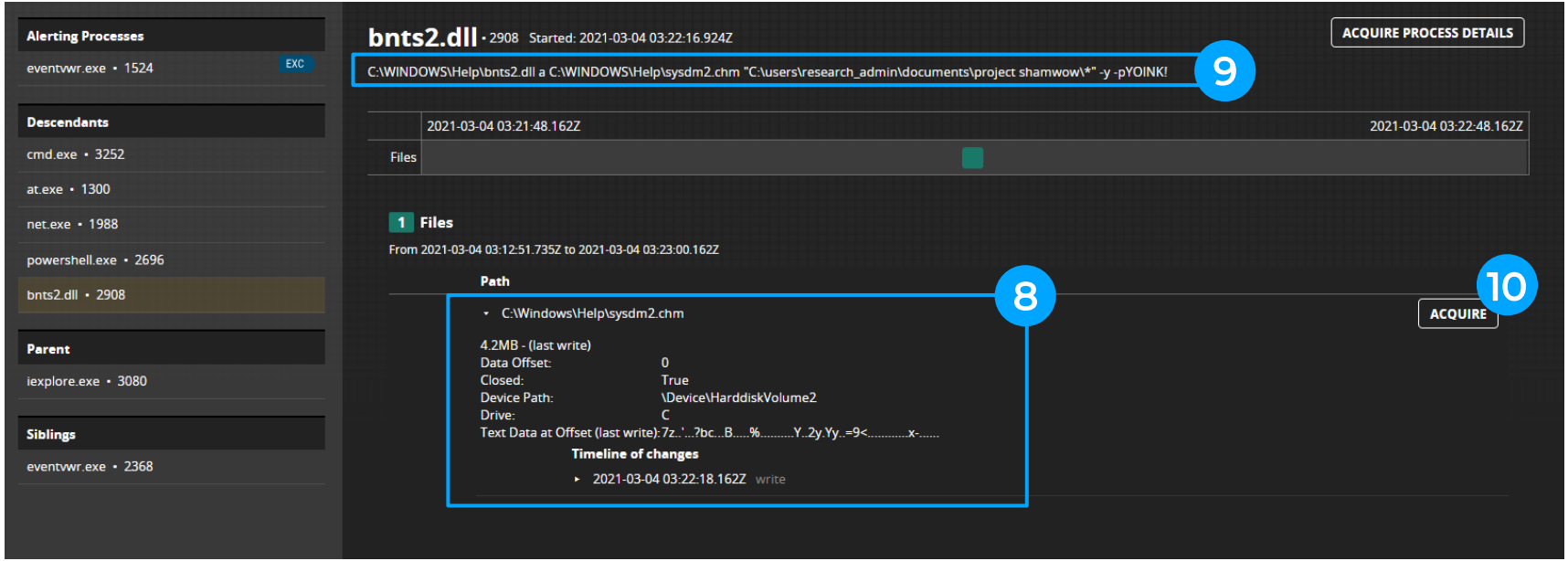
Trellix

Resumen del Triage – Archivos escritos



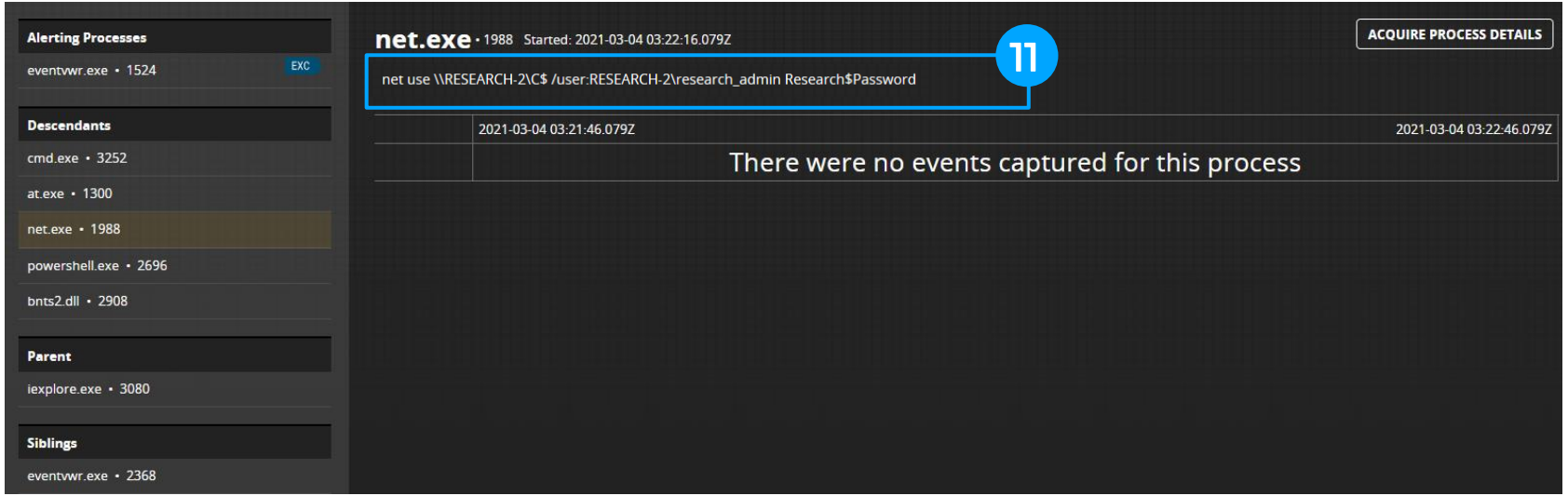
Trellix

Resumen del Triage – Archivos disfrazados



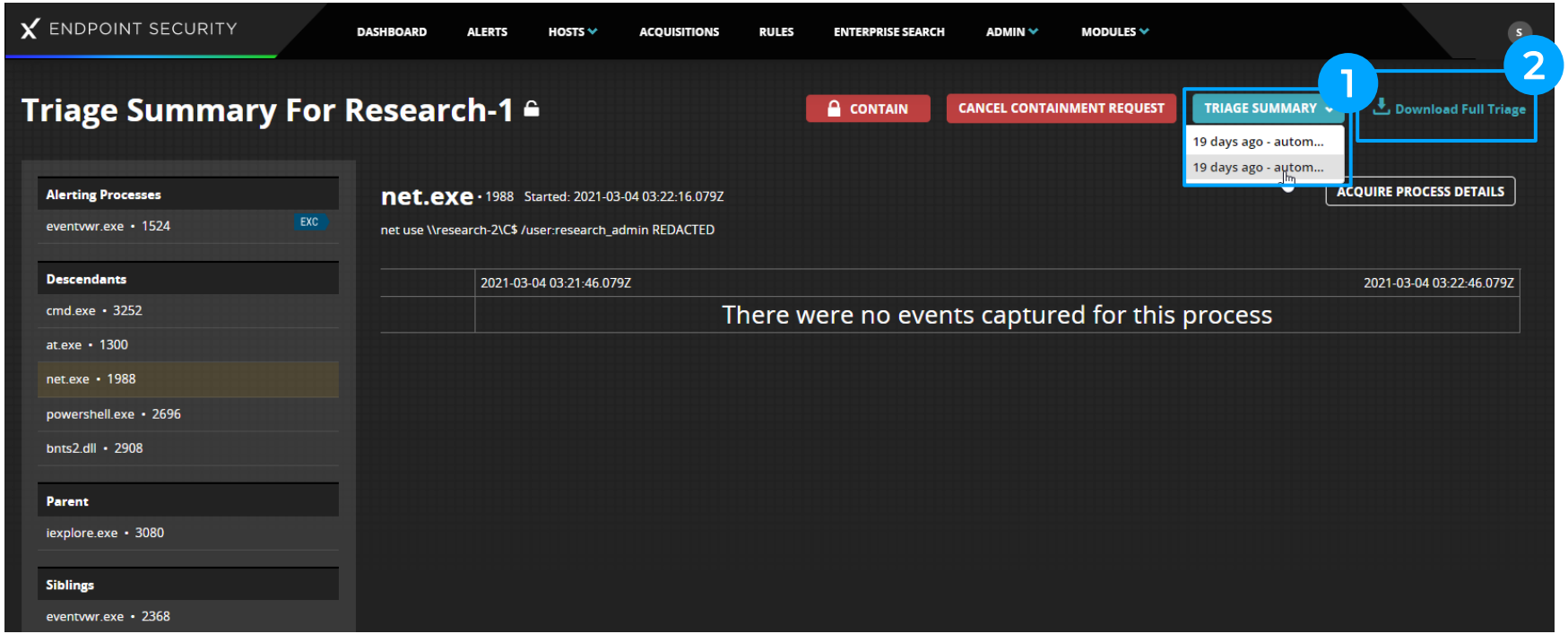
Trellix

Resumen del Triage – Movimiento lateral



Trellix

Continuación de la investigación

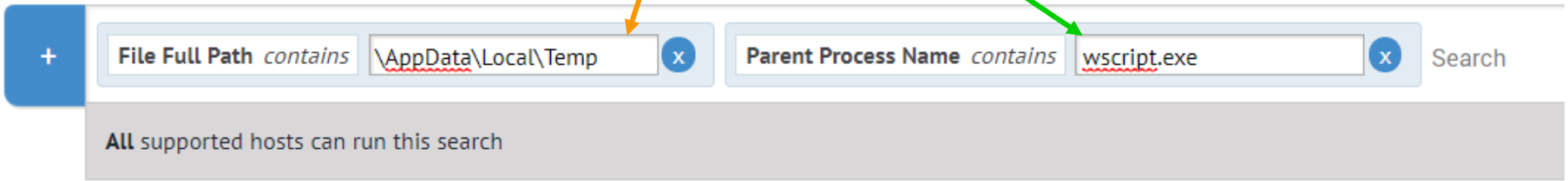


Trellix

Defining IOCs

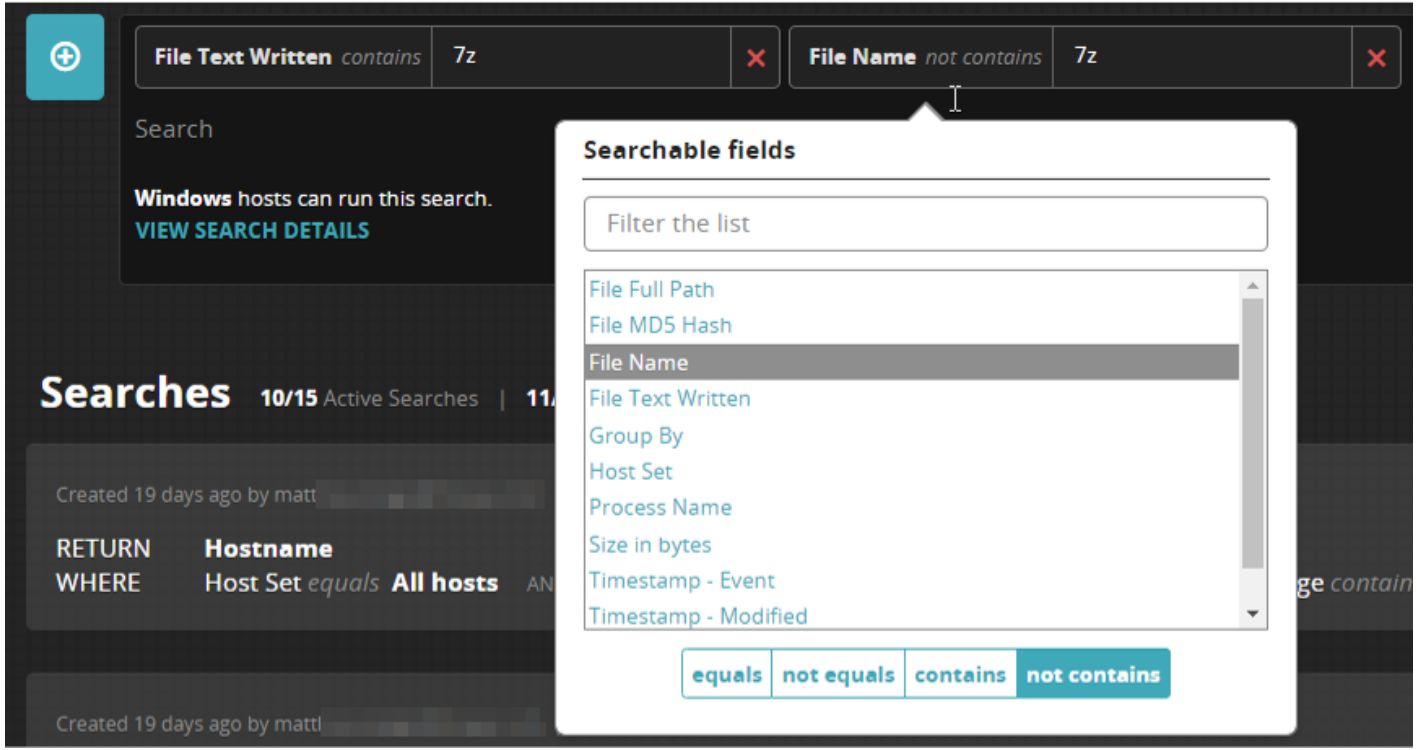
Buscando IOCs

Process	Started	C:\Users\admin\AppData\Local \Temp\index.cgi.exe Parentname: C:\WINDOWS\wscript.exe Command Line: " C:\Users\admin\Local \Temp\index.cgi.exe " MD5: 40e5b26fa58bb3af2322d74e095[illegible]5784 SHA1: bf08a919341063a[illegible]a00787b69f99db15f0f98f687	3504	1976	15944



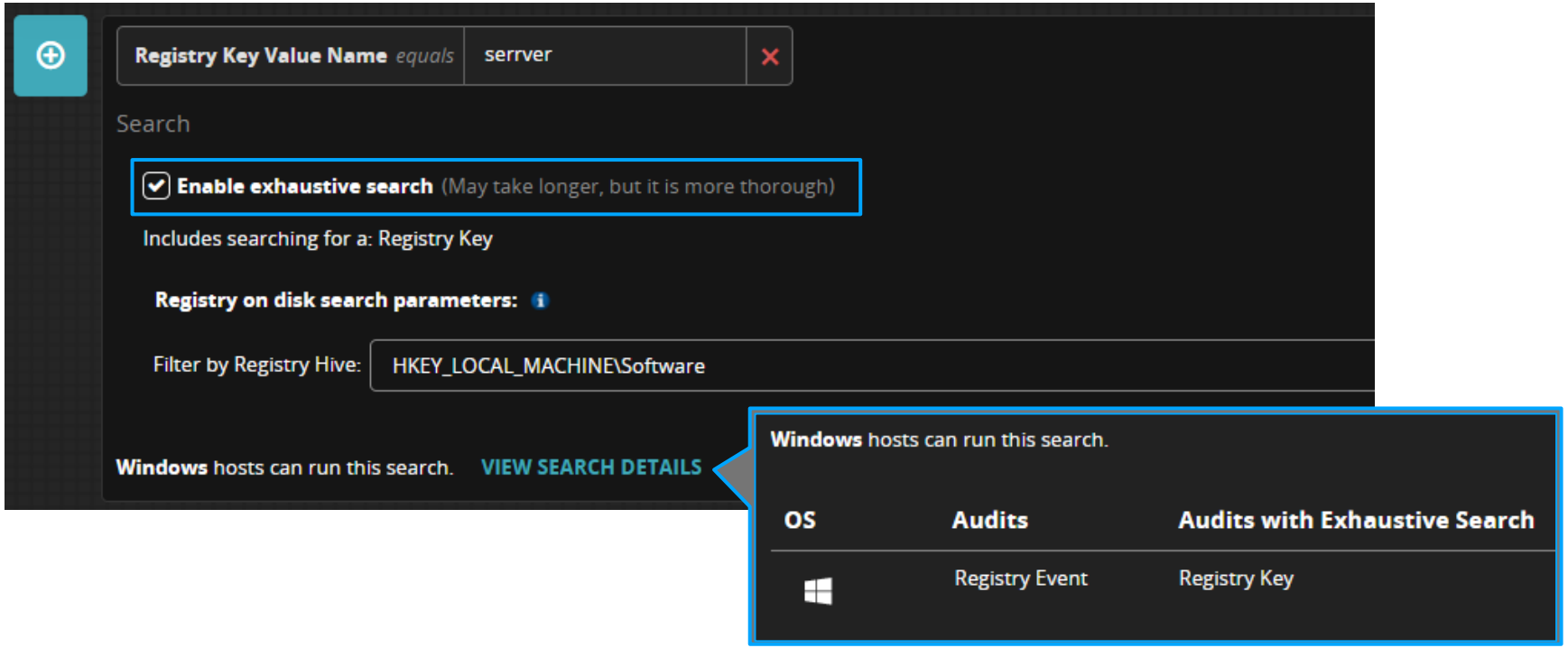
Trellix

Enterprise Search

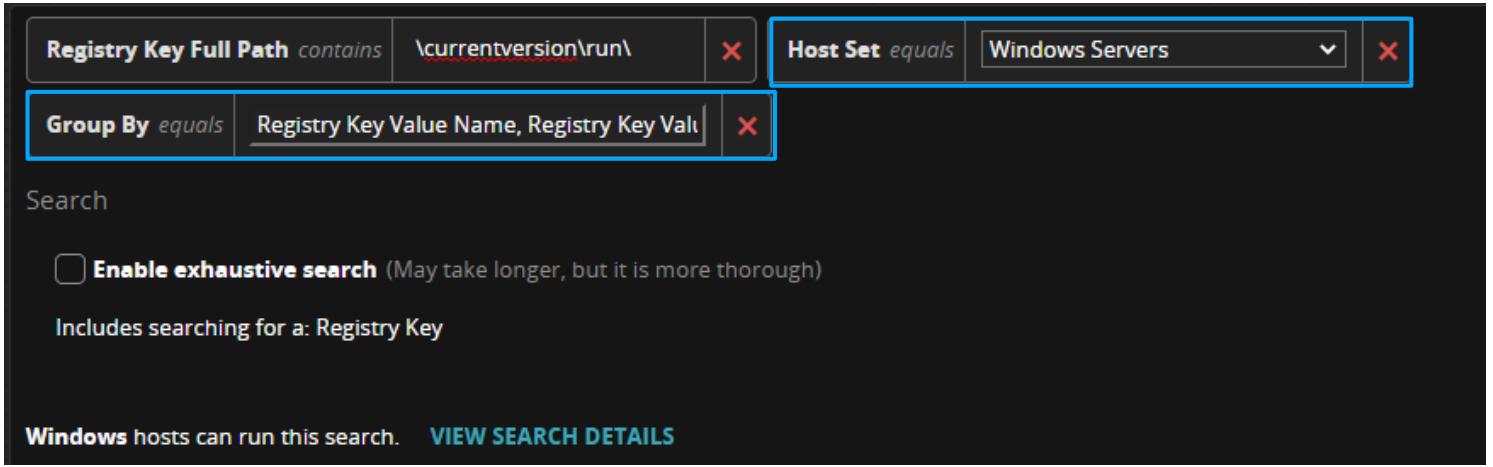


Trellix

Búsqueda exhaustiva

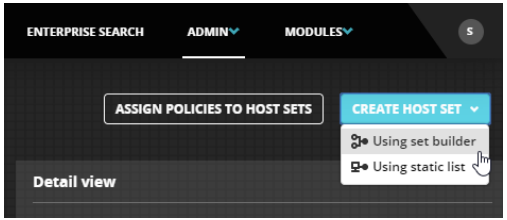


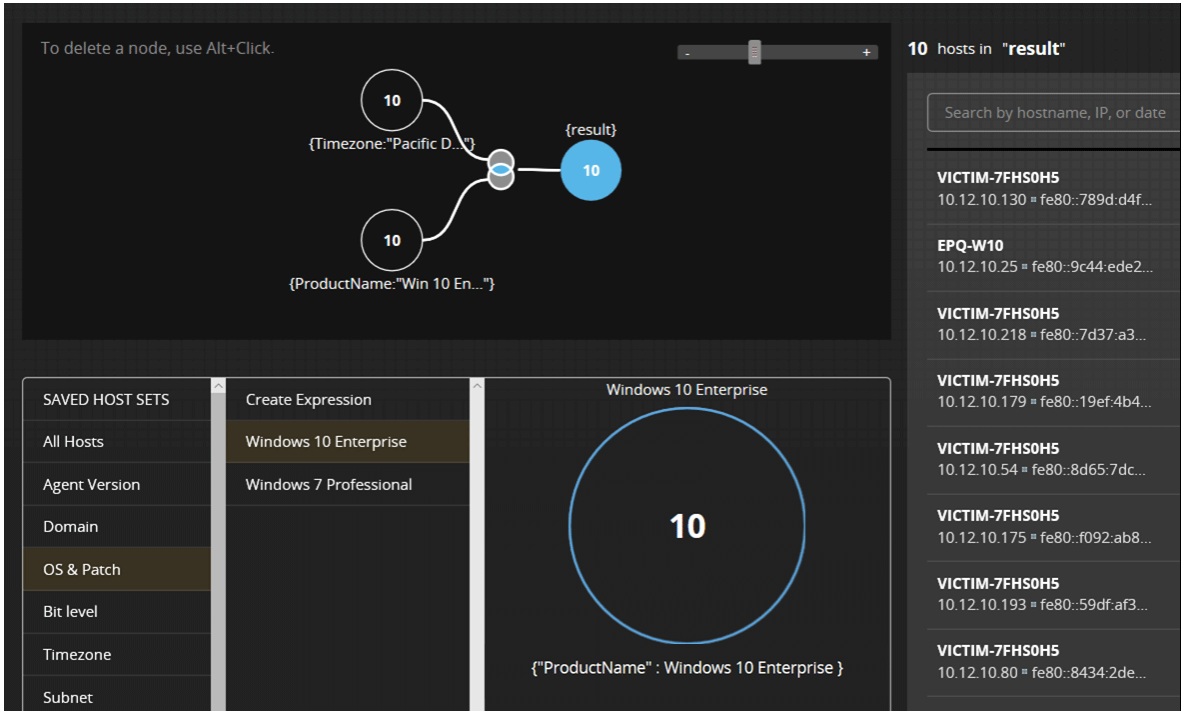
Modo de cuadrícula y búsqueda de grupos de hosts específicos



Trellix

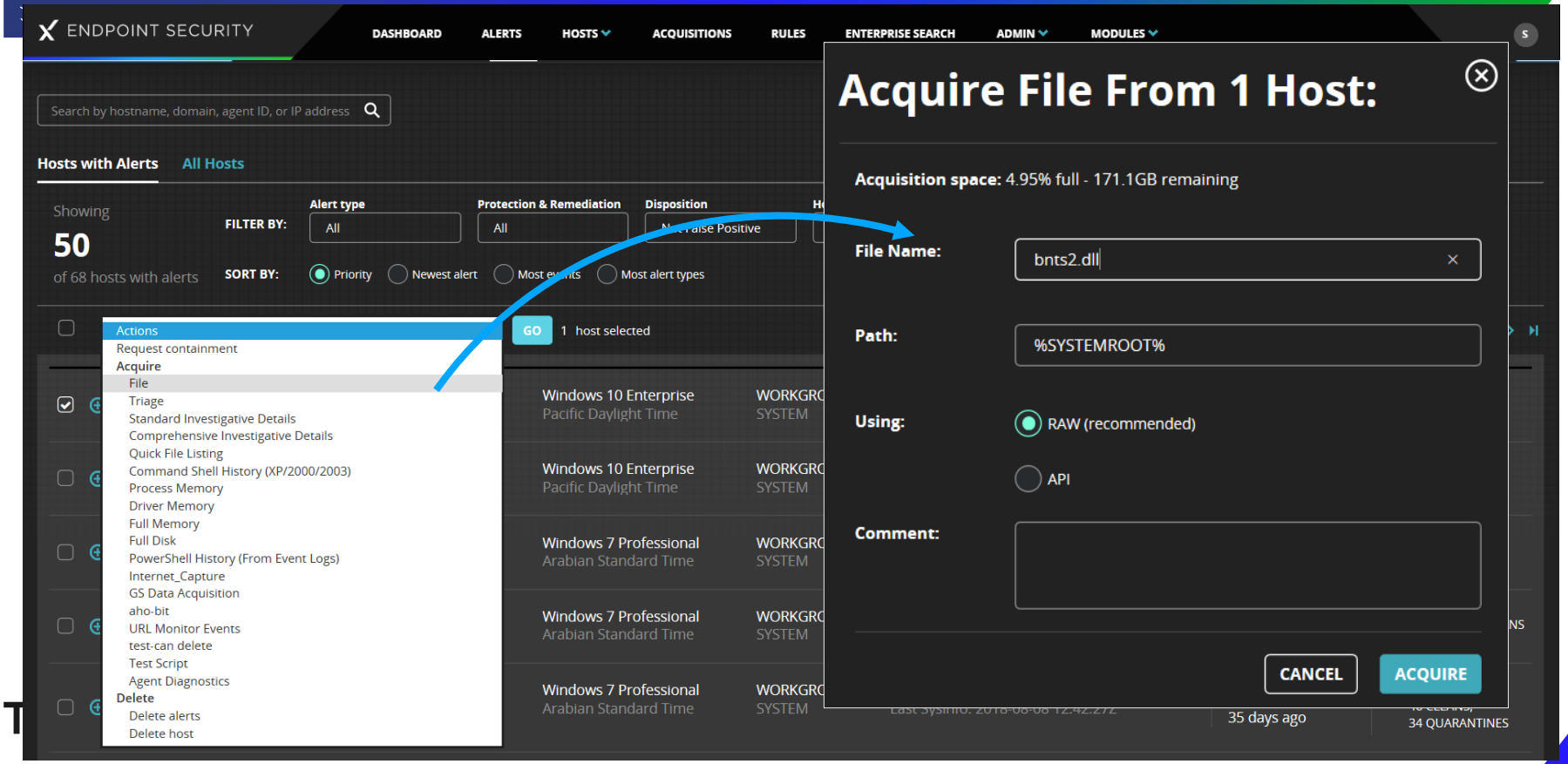
Host Sets (grupos de hosts)





Trellix

Adquisiciones



DEMO

Trellix

Thank you for your

Participation

Trellix


Trellix