Bitdefender®

Cloud Security for Endpoints

Formación técnica

Agenda

1. **Descripción de las soluciones corporativas de Bitdefender**
2. **Cloud computing y los nuevos productos de seguridad cloud**
3. **Infraestructura de seguridad cloud y modelos de servicios**
4. **Cloud Security for Endpoints**
    - 4.1 Arquitectura de Cloud Security for Endpoints
    - 4.2 Requisitos del sistema (Console y Endpoint)
    - 4.3 Cloud Security Console y mecanismo de inicio de sesión
    - 4.4 Tipos de cuentas (usuario)
    - 4.5 Descripción de la interfaz
    - 4.6 Descripción del panel y portlets del panel (informes)
    - 4.7 Organización de equipos
        - Añadir clientes
        - Preparar la instalación
    - 4.8. Área de instalación
        - Instalación manual (Console y Endpoint)
        - Instalación remota (Console y Endpoint)
    - 4.9 Ver equipos

Agenda

4.10 Endpoint Client – Configuración de usuario y paneles
4.11 Endpoint Client – Eventos
4.12 Endpoint Client – Desinstalar
4.13 Políticas
- Resumen de plantillas predeterminadas
- Crear y aplicar políticas

4.14 Informes
- Crear informes
- Ver informes
- Informes de estado de actualización y estado del equipo

4.15 Cuarentena
4.16 Registros
4.17 Licencias
4.18 Resolución de problemas – Validar la instalación
4.19 Detalles de los servicios de Endpoint Client
4.20 Ayuda y Soporte

5. Cloud Security for Endpoints vs. Bitdefender Client Security v.3.5

1. Descripción de las soluciones corporativas de Bitdefender

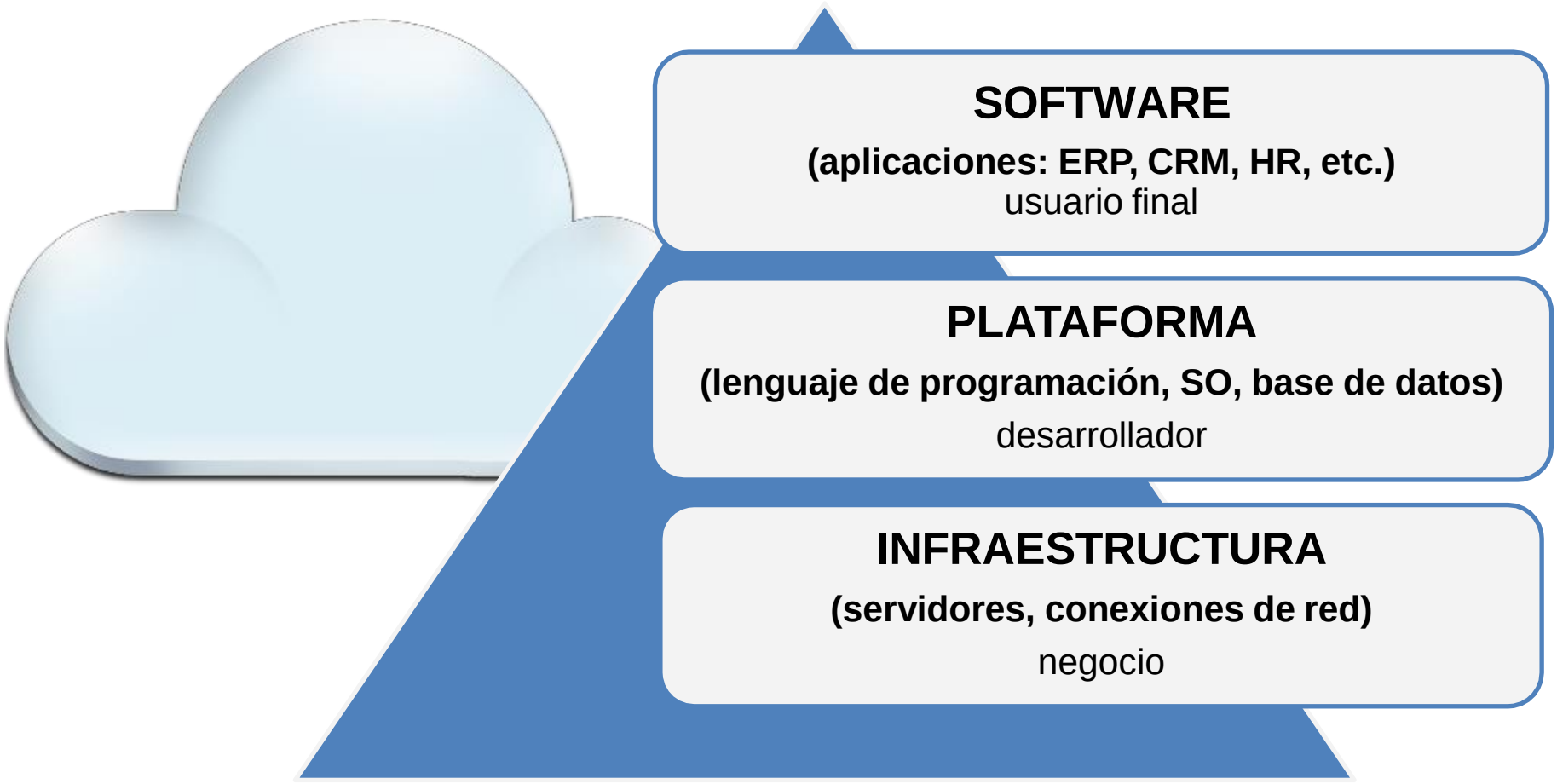
- **SOLUCIONES ACTUALES ON-PREMISE**
  - Administración centralizada v.3.5
  - Endpoint protection v.3.5
    - Bitdefender Client Security
    - Bitdefender Antivirus for Mac
    - Bitdefender Antivirus Scanner for Unices
  - Critical Server Protection v.3.5
    - BitDefender Security for File Servers
    - Bitdefender Security for Samba
    - Bitdefender Security for SharePoint
  - Gateway Services Protection v.3.5
    - Bitdefender Security for Mail Servers
    - Bitdefender Security for Exchange
    - Bitdefender Security for ISA Servers (v. 2.4)

- **GRAVITY ARCHITECTURE**
  - Cloud Security for Endpoints (octubre 2011)
  - Cloud Security for E-mail (diciembre 2011)
  - Security for Virtualized Environments (octubre 2011)

- **FUTURAS SOLUCIONES ON-PREMISE** basadas en la nueva Gravity Architecture (2012)

2. Cloud computing

- Usar tecnología online, servicios y software online.
- Tecnología informática que usa Internet y los servidores remotos para mantener los datos y las aplicaciones.
- Informática bajo demanda.



2. Informática convencional frente a cloud

	Informática convencional	Cloud computing
TIEMPO DE CONFIGURACIÓN	De días a semanas	Minutos
COSTES	Costoso (mucha inversión), costes elevados para la adquisición de servidores se usen o no	Sin costes anticipados, pago por uso, alquiler de servidores basados únicamente en el uso
LO QUE NECESITA	Centro de datos con seguridad Suministro de refrigeración y eléctrico Servidores y almacenamiento Licencias del SO Parches de software y seguridad Actualización del software Actualizaciones de equipos Downgrades Suministro energético para backup Desarrollo, Pruebas, Producción Fail over Recuperación ante desastres Espacio en rack Soporte Mantenimiento Replicación	**Se necesita CONEXIÓN A INTERNET** **No** es necesario comprar servidores y hardware **No más** cajas **No más espacio** en rack **Se acabaron** los costosos ingenieros para el soporte y mantenimiento **Sin** recursos malgastados - Seguridad - Fiabilidad - Escalabilidad

2. Los nuevos productos de seguridad cloud

Cloud Security for Endpoints

- Cliente discreto
- Estaciones de trabajo Windows y servidores
- Seguridad Web y control
- Cortafuego con control de usuario
- Políticas basadas en grupos
- El diseño modular permite introducir nuevas características

Consola de Seguridad Cloud

- Consola basada en Web
- Controles de acceso granulares
- Panel configurable
- Integración de Active Directory
- Instalación remota
- Widgets de presentación de informes
- Políticas de seguridad y actualización

Cloud Security for Email

- Seguridad de correo alojada externamente
- Reglas del filtro de contenido
- Antimalware integrado
- Motor antispam líder
- Administración de la cuarentena
- Presentación de informes detallada
- Integrado con Cloud Security Console

3. Infraestructura de seguridad en la nube global

1. Diseñado para reducir el impacto general en los costes de TI asociados
2. Diseñado para alcanzar una disponibilidad del 100%
3. Respaldado por un acuerdo de nivel de servicio (SLA)
4. Usa centros de datos de alta seguridad
5. Centros de datos ubicados en los principales continentes
6. Utiliza tecnologías de balanceo de carga y failover

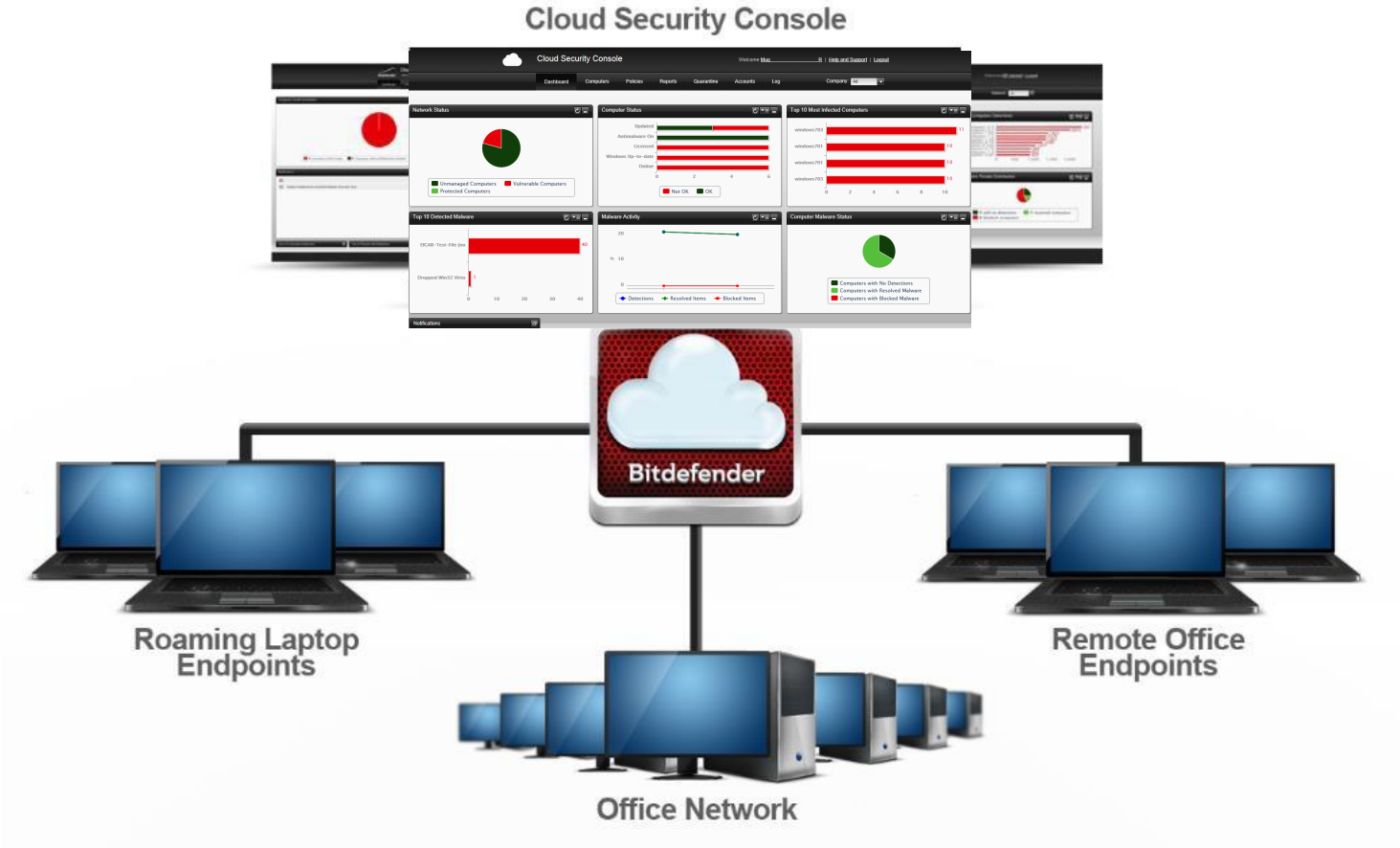
3. Modelos de servicio cloud

Gravity Architecture da una oportunidad a cada empresa:

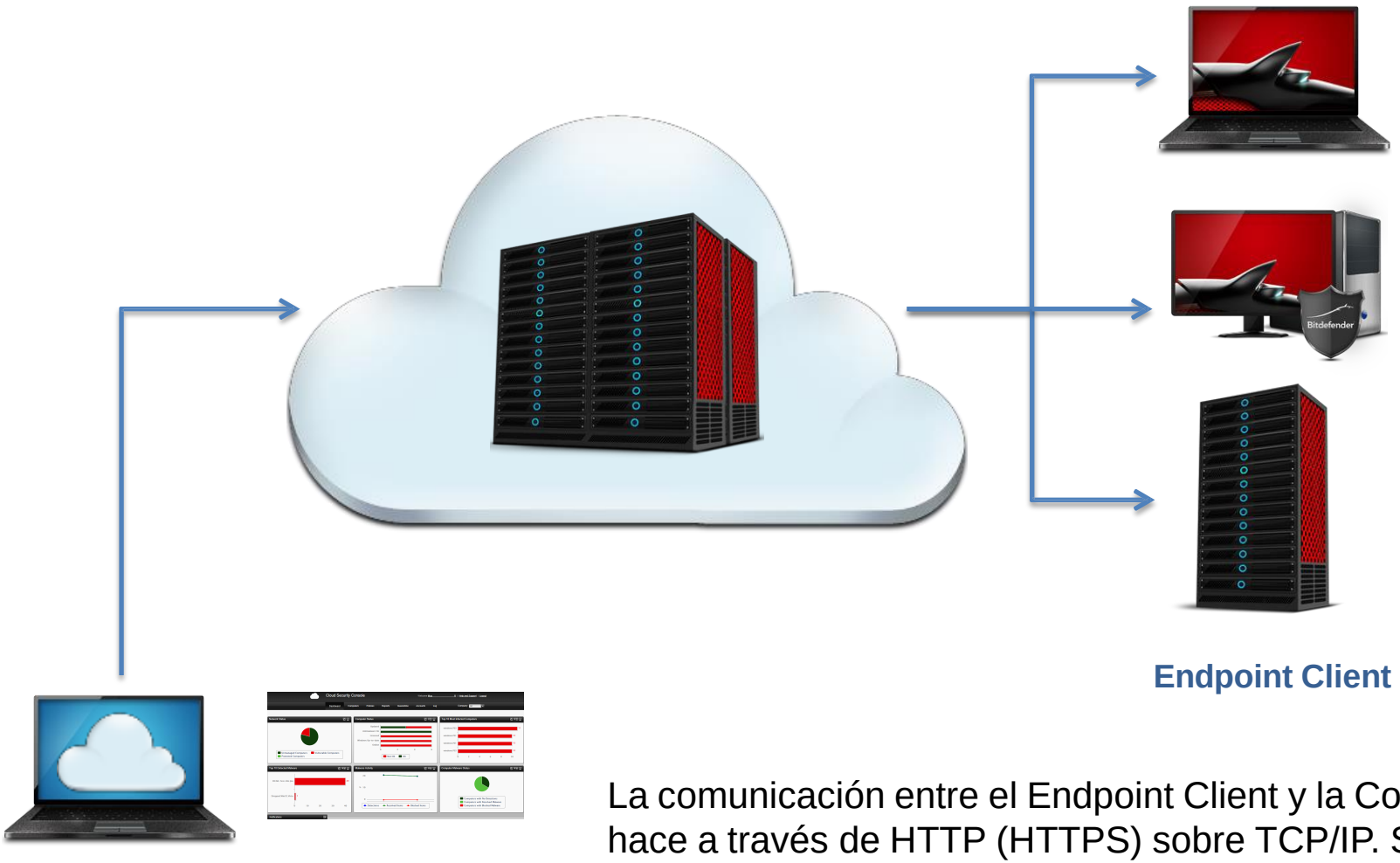
1. **Nube pública** ideal para las pequeñas empresas para proteger de 2 a 100 puntos finales
2. **Nube privada** ideal para que empresas medianas y grandes protejan una ubicación
3. **Nube híbrida** ideal para empresas medianas y grandes con múltiples ubicaciones

4. Cloud Security for Endpoints

Cloud Security for Endpoints protege sistemas utilizando una tecnología de seguridad reconocida una y otra vez como la número uno. No requiere de hardware en el sitio y se administra desde Cloud Security Console, una potente e intuitiva interfaz para una solución que defiende sus sistemas, para cualquier número de puntos finales y defendiéndolos desde cualquier lugar.



4.1 Cloud Security for Endpoints – Arquitectura



Endpoint Client

Cloud Security Console

La comunicación entre el Endpoint Client y la Consola/Servidor se hace a través de HTTP (HTTPS) sobre TCP/IP. Se usa el protocolo SSL.

4.2 Requisitos del sistema

Cloud Security Console (la consola basada en Web)

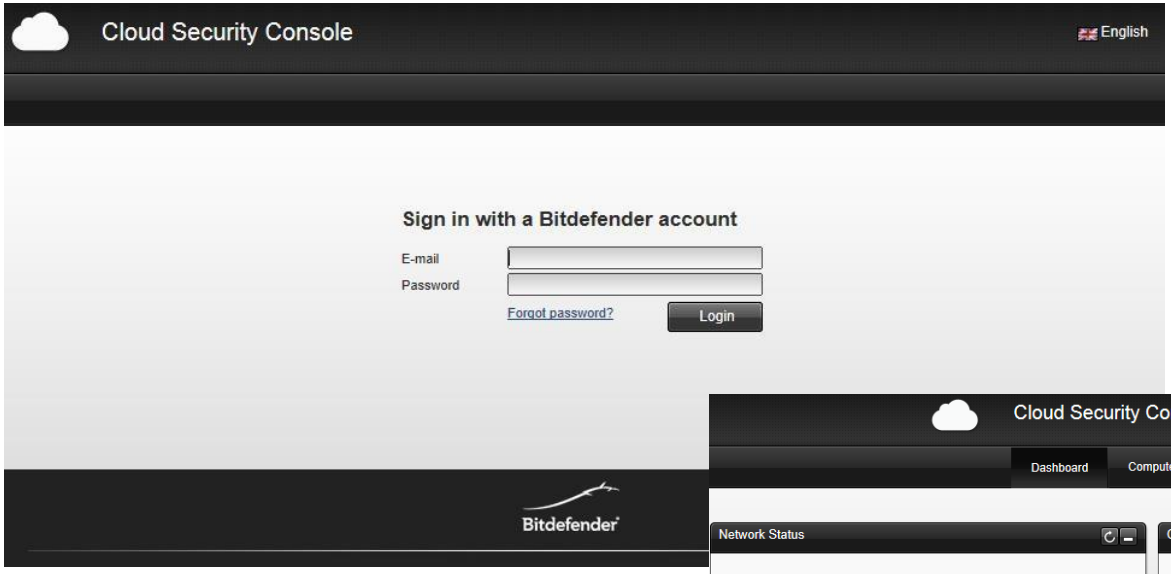
- Se necesita conexión a Internet
- Internet Explorer 8 o superior
- Firefox 4 o superior
- Google Chrome 8 o superior
- Safari 5.0.4 o superior

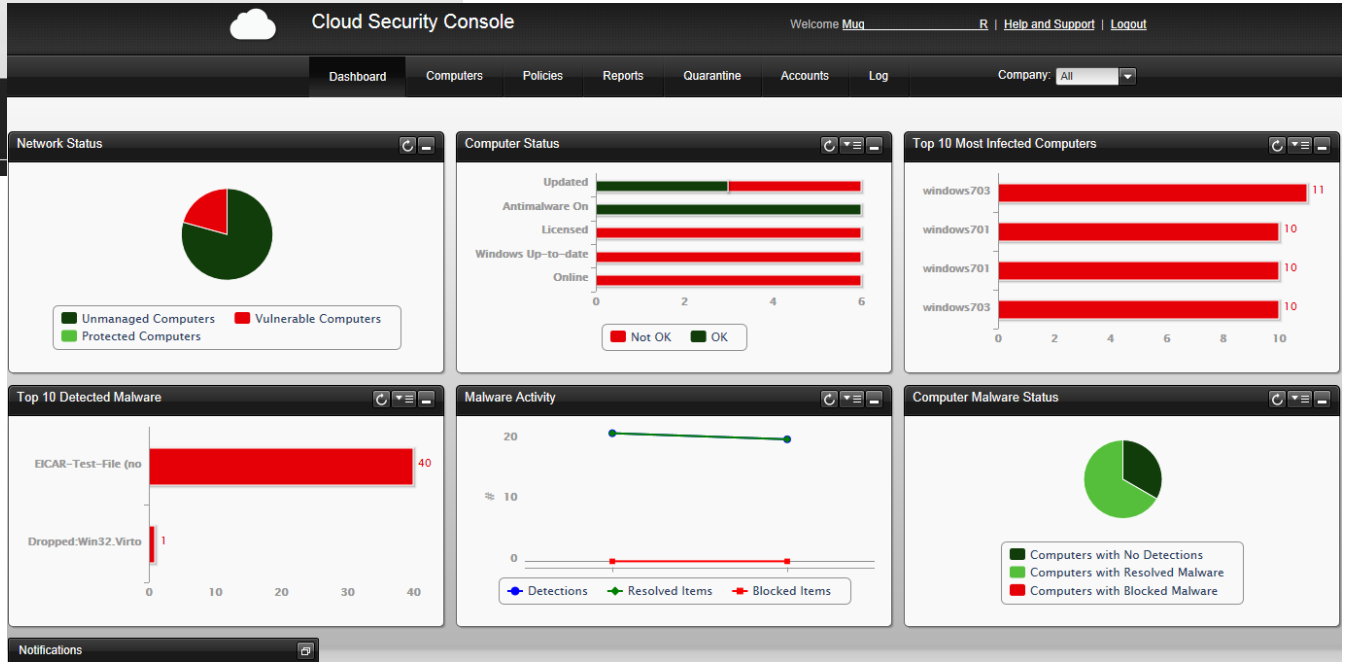
Endpoint Client (el programa de seguridad informática totalmente automatizado)

- Indicado para estaciones de trabajo, portátiles y servidores que se ejecuten en MS Windows
- **Estación de trabajo**: Windows 7, Vista (SP1), XP (SP3), Embedded Standard 7
- **Servidor**: Windows SBS 2011, 2008 R2 / SBS, 2003 SP1 / R2 / SBS, Home Server
- **CPU**: compatible Intel® Pentium (32/64-bits), 800 MHz (Windows XP), 1 GHz (Windows Vista, Windows 7), 1.5 GHz (Windows Servers)
- **Memoria**: 256 MB (Windows XP), 1 GB (Windows 7, Vista, 2008, 2003), 1,5 GB (SBS 2003), 4 GB (SBS 2008), 8 GB (SBS 2011)
- **Disco duro**: 1 GB
- **Conexión a Internet**: Internet Explorer 7+, Mozilla Firefox 4+, Google Chrome, Safari u Opera para la seguridad del navegador del punto final.

4.3 Cloud Security Console

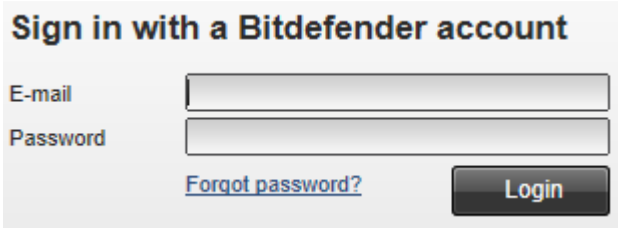
Se usa una interfaz Web central para instalar, configurar, monitorizar e informar sobre el estado de seguridad de los centros de datos y sistemas de usuario final.



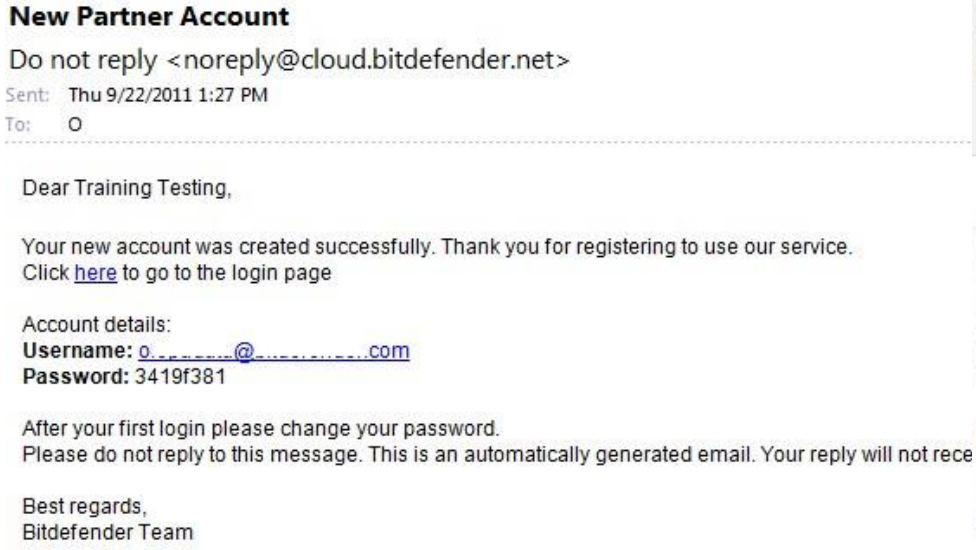


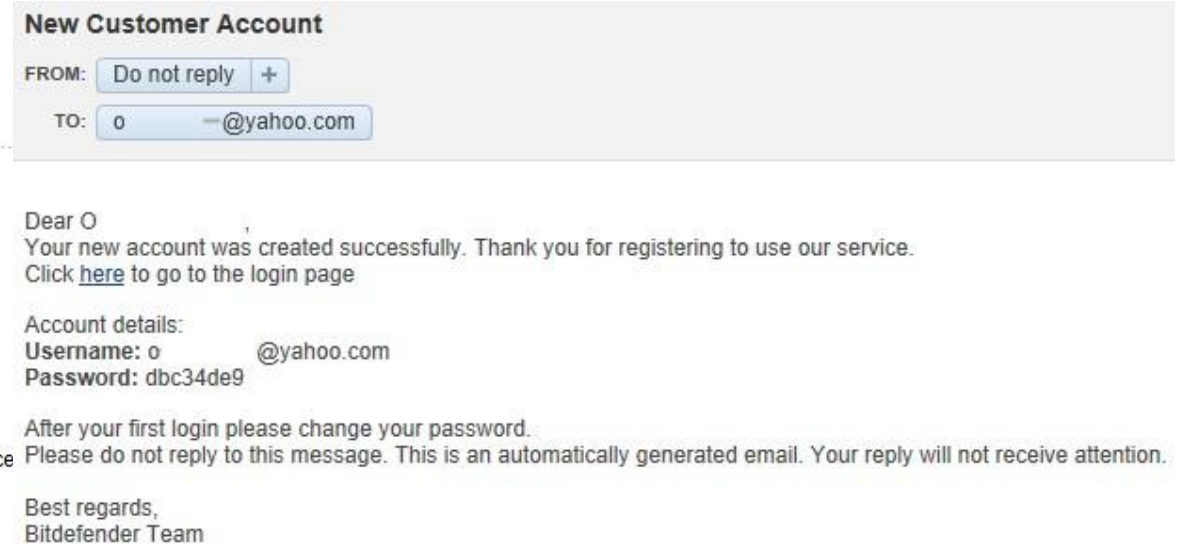
4.3. Mecanismo de inicio de sesión

ENLACE para acceder a Cloud Security Console:
https://cloud.bitdefender.net/

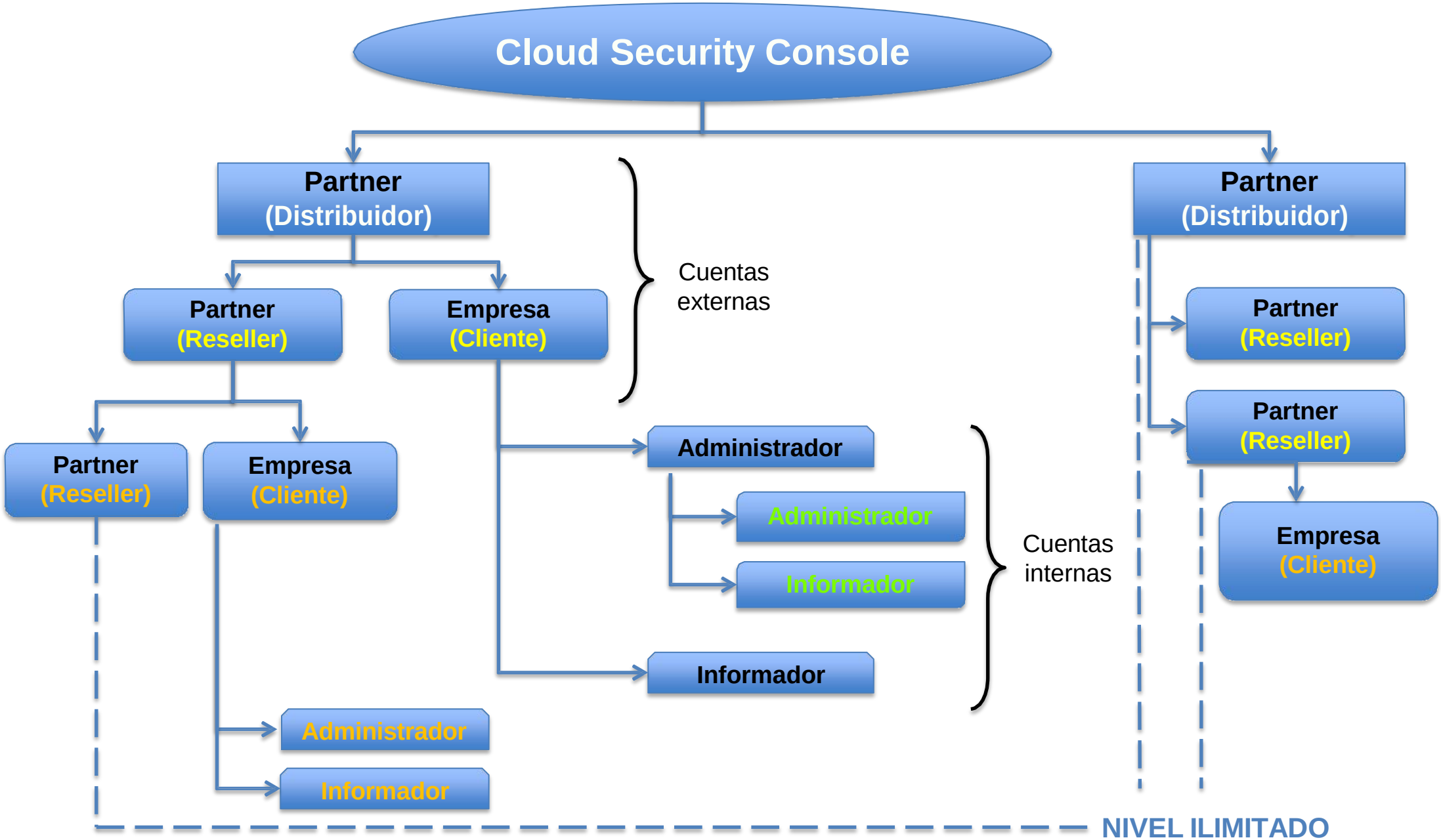


- Para los **PARTNERS**: las cuentas las crea el personal de Bitdefender u otros partners
- Para **CLIENTES**: las cuentas las crean los partners
- Para ambos, los datos de inicio de sesión y credenciales se envían por e-mail





4.4 Tipos de cuentas (usuario)



4.4 Tipos de cuentas (usuario)

Cuentas PARTNER

Con una cuenta partner puede crear otras cuentas "partner" tales como cuentas para VARs, distribuidores, etc., y por supuesto cuentas cliente que puede listar por empresas. Con esta cuenta, un partner puede administrar todos sus clientes al mismo tiempo.

Cuentas CLIENTE (agrupadas bajo Empresas)

Las cuentas cliente tienen acceso únicamente a su propia red. La empresa puede administrarla un partner. Con una cuenta cliente puede crear:

- **Cuentas de administrador** – son básicamente cuentas que pueden usarse para crear otras cuentas de administrador o de informador. Estas cuentas se emplean para delegar responsabilidades para partes específicas de la red.

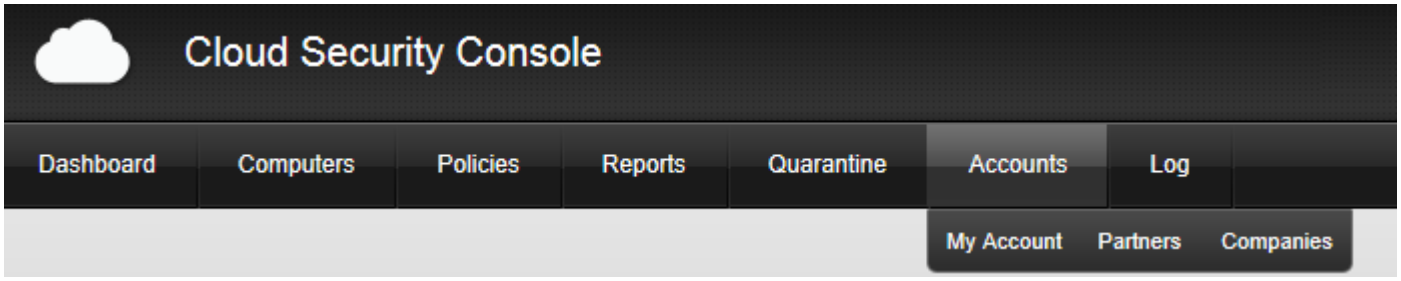
- **Las cuentas de informador** – tendrán acceso únicamente al panel de control de la consola y a la sección de informes. Estas cuentas se utilizan para el estado de seguridad e informes y no tienen acceso alguno a la configuración de seguridad de la red.

Siempre existirá una cuenta cliente por empresa.

4.5 Descripción de la interfaz

INTERFAZ disponible en 4 idiomas: English Française Español Deutsch

Interfaz para cuentas **PARTNER** (al menos una vez que se ha creado un cliente)



Interfaz para **CLIENTE** (o cuenta de **Administrador**)

Interfaz para **CLIENTE** (cuenta de **Informador**)

4.5 Descripción de la interfaz

Cuenta **PARTNER**

Cuentas

- Mi cuenta (editar la cuenta, cambiar la contraseña, establecer la zona horaria, idioma, el logo de la empresa)
- Partners (ver partners por empresas, añadir nuevos partners, activar o cancelar cuentas)
- Empresas (ver empresas, información de licencia, posibilidad es de edición y borrado, actualización y estado de malware)

Registro (muestra los registros de actividad)

Cuenta **CLIENTE** (Administradores)

Panel de control (organizado en 7 portlets, informa sobre los distintos aspectos de la seguridad de la red)

Equipos

- Ver equipos (muestra los equipos administrados y no administrados de una red específica, acceso a los informes, tareas)
- Área de instalación (opciones de instalación de Endpoint Client: instalación manual y remota, personalizar paquete)
- Ver tareas (lista de tareas, opciones de eliminación de tareas)

Políticas

- Nueva política (creación de nuevas políticas basadas en la plantilla de política predeterminada)
- Ver políticas (mostrar y eliminar las políticas creadas)

Informes

- Nuevo informe (creación de nuevos informes: tipo de informe, objetivo, repetición, intervalo de actualización)
- Ver informes (muestra los informes creados)
- Informes programados (muestra los informes programados)

Cuarentena (muestra las amenazas en cuarentena, rutas y acciones)

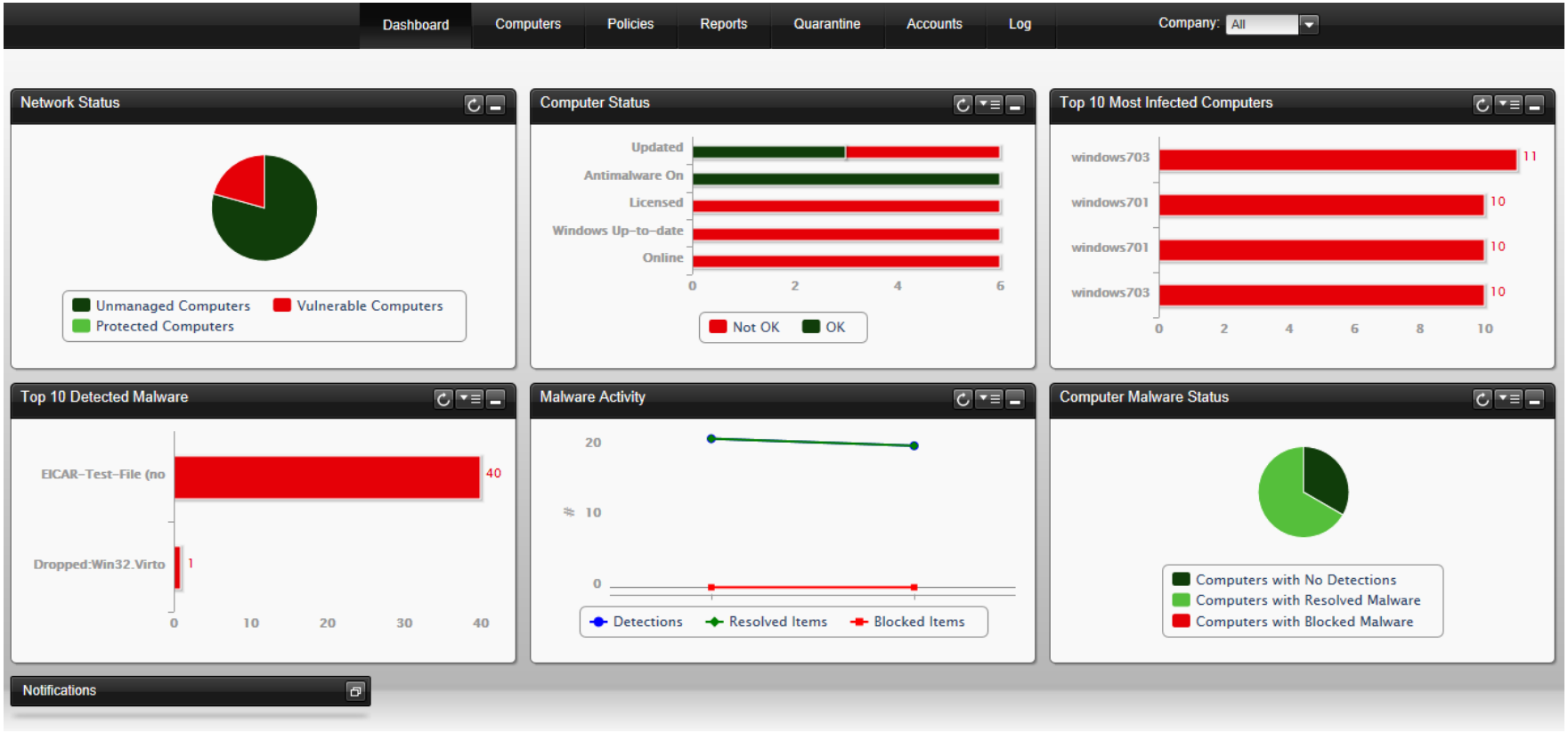
Cuentas

- Mi Cuenta (editar la cuenta, cambiar la contraseña, información de licencia, establecer la zona horaria, el idioma y cambiar el logo de la empresa)
- Usuarios (posibilidad de crear / eliminar otros usuarios, asignarles funciones de administrador o informador)

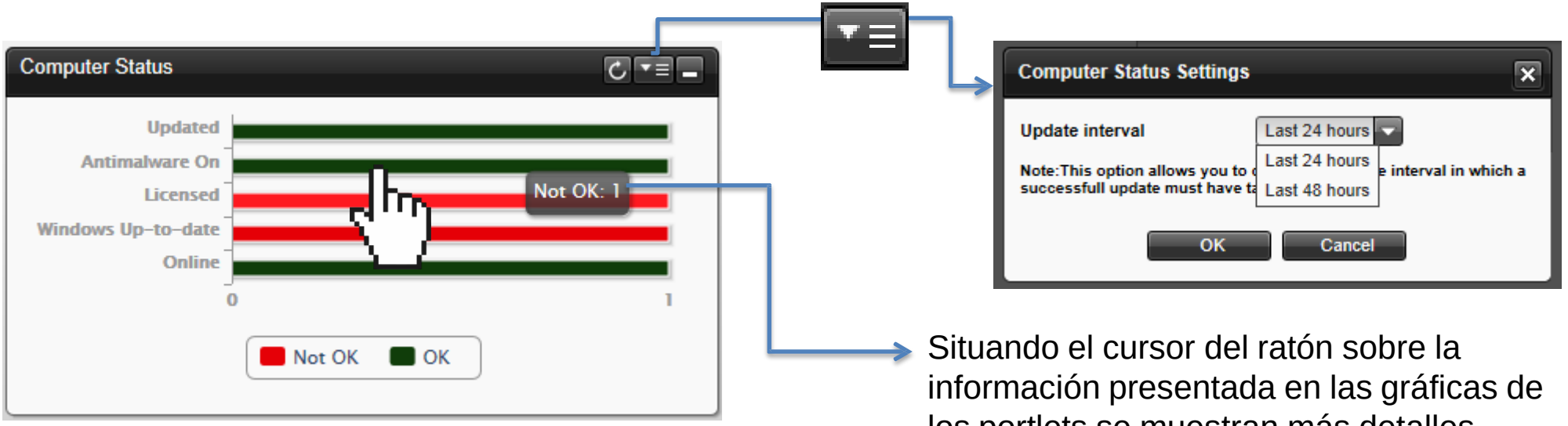
Registro (registro de actividad por usuario)

4.6 Descripción del Panel de control

El sencillo **Panel de control basado en la nube** es un panel de estado compuesto por 7 portlets que permite supervisar rápidamente la seguridad de los puntos finales protegidos, incluyendo tanto equipos como servidores, con actualización continua de informes locales de múltiples redes o ubicaciones dispersas geográficamente. El panel de seguridad es fácil de configurar basándose en las preferencias particulares y proporciona también una visión general de las amenazas de seguridad globales.

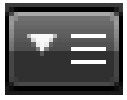


4.6 Descripción del Panel de control – Portlets



Situando el cursor del ratón sobre la información presentada en las gráficas de los portlets se muestran más detalles

Actualizar (actualización de datos independiente para cada portlet)



Opciones (algunos de los portlets ofrecen más opciones)

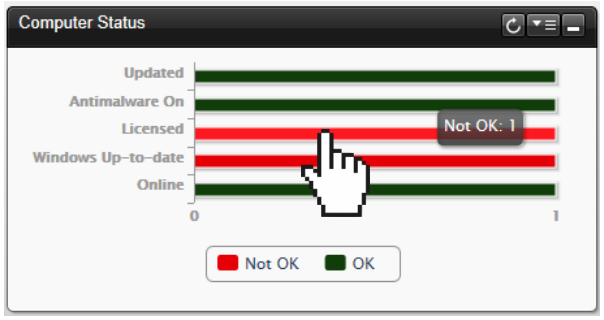
Minimizar (puede minimizar los portlets y los restantes se ajustarán automáticamente para adaptarse a la pantalla)

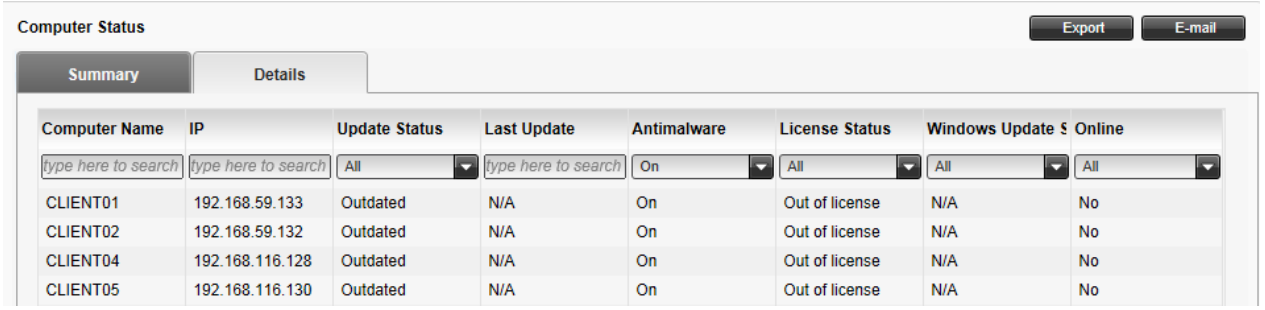
Restaurar (restaura los paneles minimizados)

Acceso al informe (haciendo clic en una gráfica se mostrará el informe filtrando los datos a los que ha accedido)

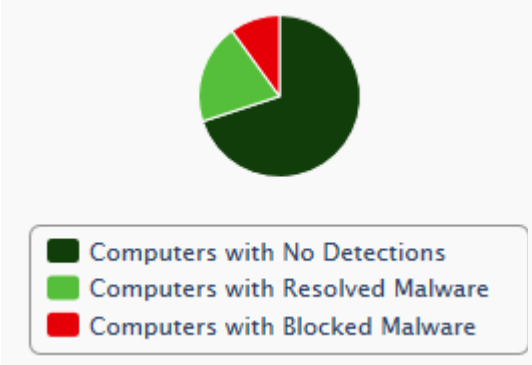
4.6 Descripción del Panel de control – Portlets

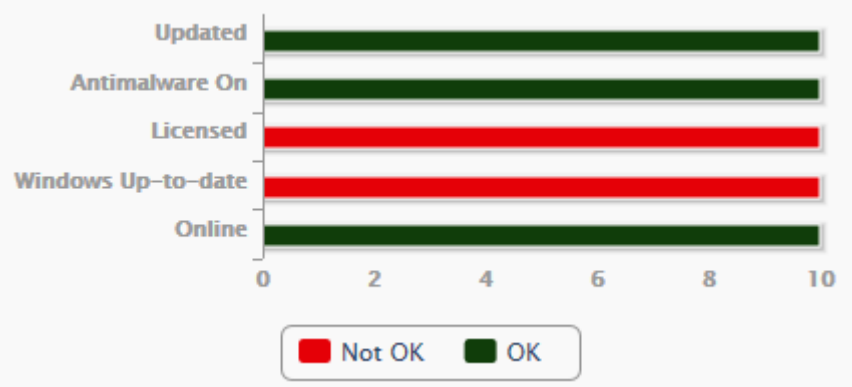
Todos los portlets del Panel de control tienen un **INFORME** asociado, de forma que cuando se accede al diagrama / gráfico, será redirigido al área de informes, donde aparecerá automáticamente un informe, mostrándole información filtrada relacionada con la selección que realizó.





Hay disponibles distintos tipos de informes, de manera que pueda encontrar fácilmente y administrar la información que necesita. La información se presenta como gráficos de tarta, tablas y diagramas de fácil lectura, para permitir una comprobación rápida del estado de seguridad de la red e identificar incidencias de la seguridad.





4.6 Visión general del Panel de control – Portlets

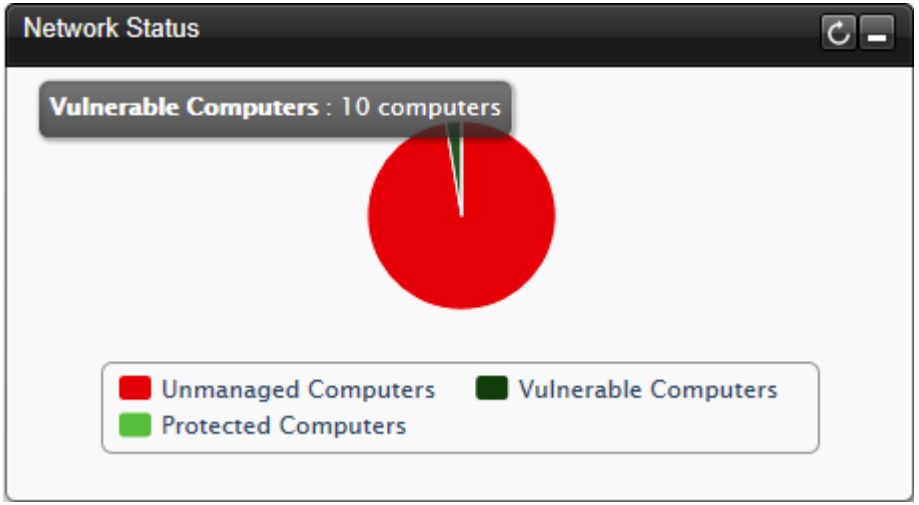
ESTADO DE LA RED

Le proporciona información detallada sobre el estado de seguridad general de los equipos seleccionados. Los Equipos se agrupan basándose en estos criterios:

- Los **equipos no administrados** no tienen instalada la protección Bitdefender Cloud Security for Endpoints y su estado de seguridad no puede evaluarse.

- Los **equipos protegidos** tienen instalada la protección Bitdefender Cloud Security for Endpoints y no se han detectado amenazas de seguridad.

- Los **equipos vulnerables** tienen instalada la protección de Bitdefender Cloud Security for Endpoints, pero determinadas condiciones impiden la adecuada protección del equipo.

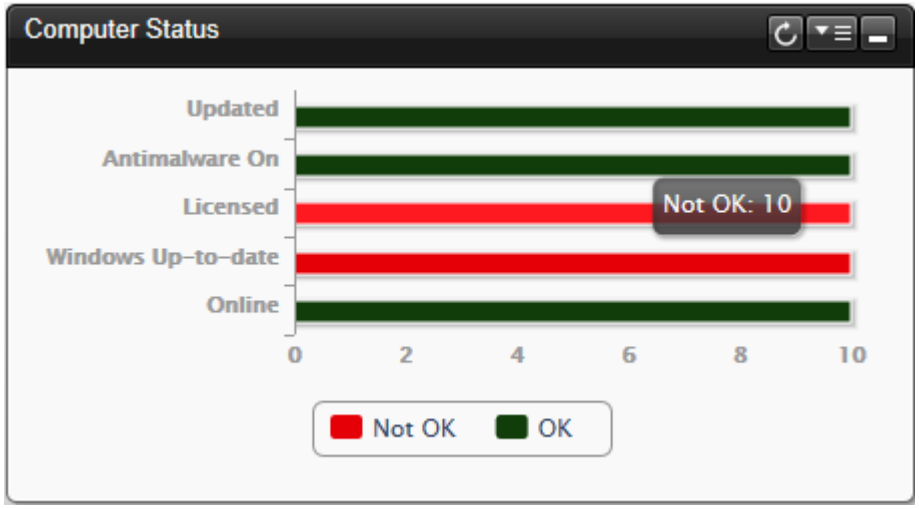


4.6 Visión general del Panel de control – Portlets

ESTADO DEL EQUIPO

Le proporciona diversas informaciones de estado relativas a los equipos seleccionados en los que se ha instalado la protección Bitdefender Cloud Security for Endpoints.

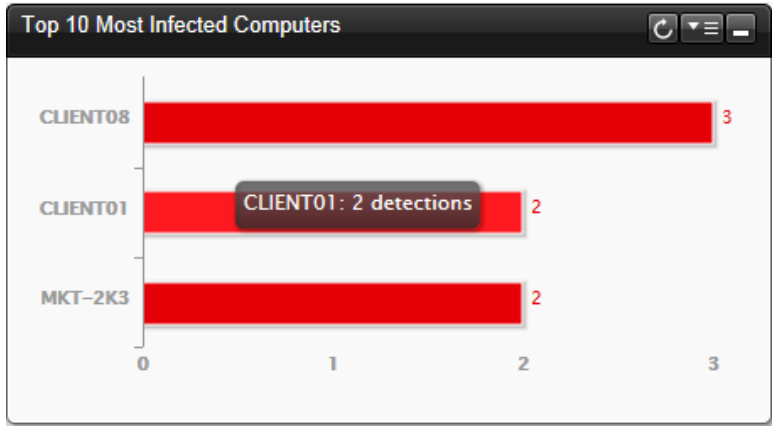
- Estado de actualización de la protección
- Estado de protección antivirus
- Estado de la licencia
- Estado de actualización de Windows
- Estado de actividad de la red (online/offline)



4.6 Visión general del Panel de control – Portlets

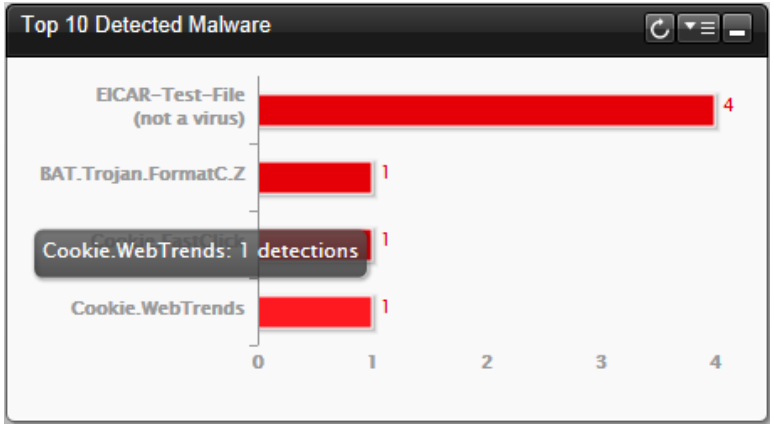
LOS 10 EQUIPOS MÁS INFECTADOS

Muestra los 10 equipos más infectados durante un periodo de tiempo específico en los equipos seleccionados



LOS 10 MALWARES MÁS DETECTADOS

Le muestra las 10 amenazas más detectadas durante un periodo de tiempo específico en los equipos seleccionados



4.6 Visión general del Panel de control – Portlets

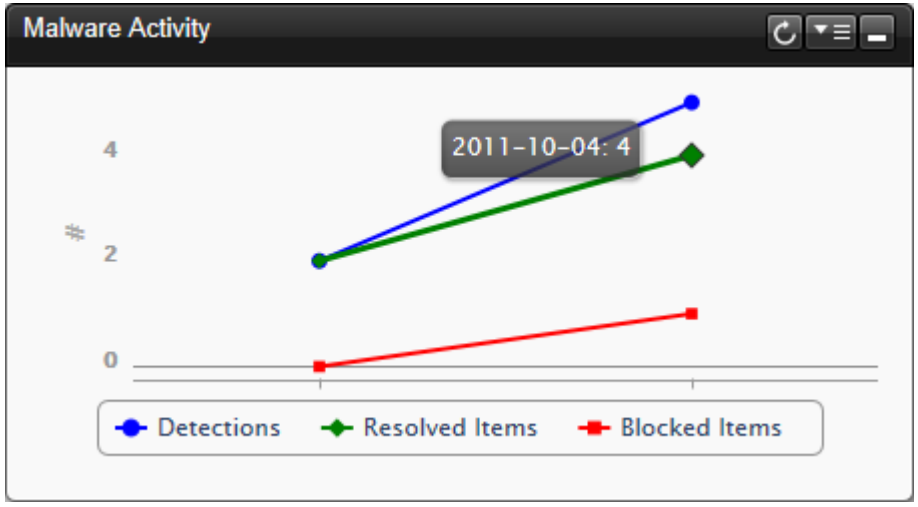
ACTIVIDAD MALWARE

Le ofrece detalles generales y por equipos de las amenazas malware detectadas durante un periodo de tiempo específico en los equipos seleccionados. Puede ver:

- Número de **detecciones** (archivos que se han encontrado infectados con malware)

- Número de **infecciones resueltas** (archivos que han sido desinfectados o aislados con éxito en la carpeta de cuarentena)

- Número de **infecciones bloqueadas** (archivos que no pudieron desinfectarse pero se ha rechazado el acceso a ellos; por ejemplo, un archivo infectado almacenado en algún formato comprimido propietario)



4.6 Visión general del Panel de control – Portlets

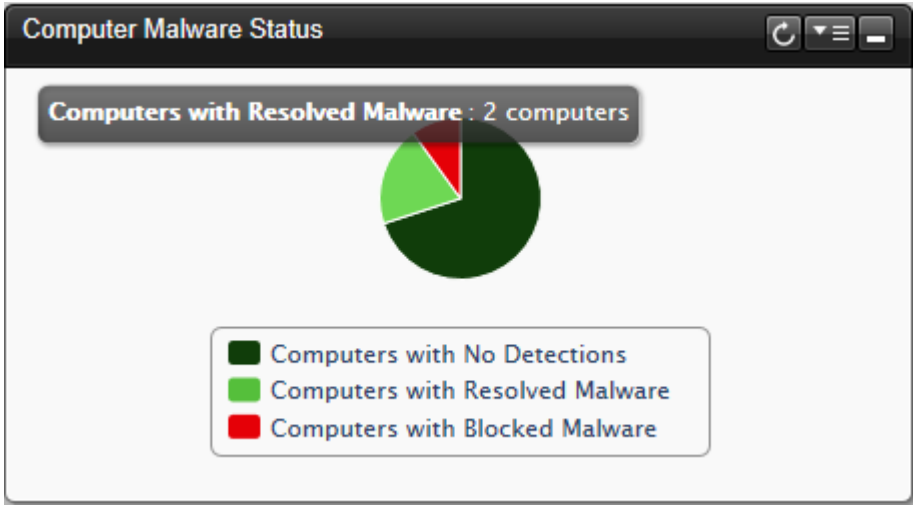
ESTADO MALWARE DEL EQUIPO

Le ayuda a encontrar cuántos y cuáles de los equipos seleccionados han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas. Los Equipos se agrupan en base a estos criterios:

- Equipos sin **detecciones** (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)

- Equipos con **malware solucionado** (todos los archivos detectados han sido desinfectados correctamente o aislados en la carpeta de cuarentena)

- Equipos con **malware bloqueado** (se ha bloqueado el acceso a algunos de los archivos detectados)



4.6 Visión general del Panel de control – Portlets

NOTIFICACIONES

Las notificaciones se envían por e-mail. Se muestran sólo cuando se cumplen las condiciones correspondientes. Se dispone de las siguientes notificaciones:

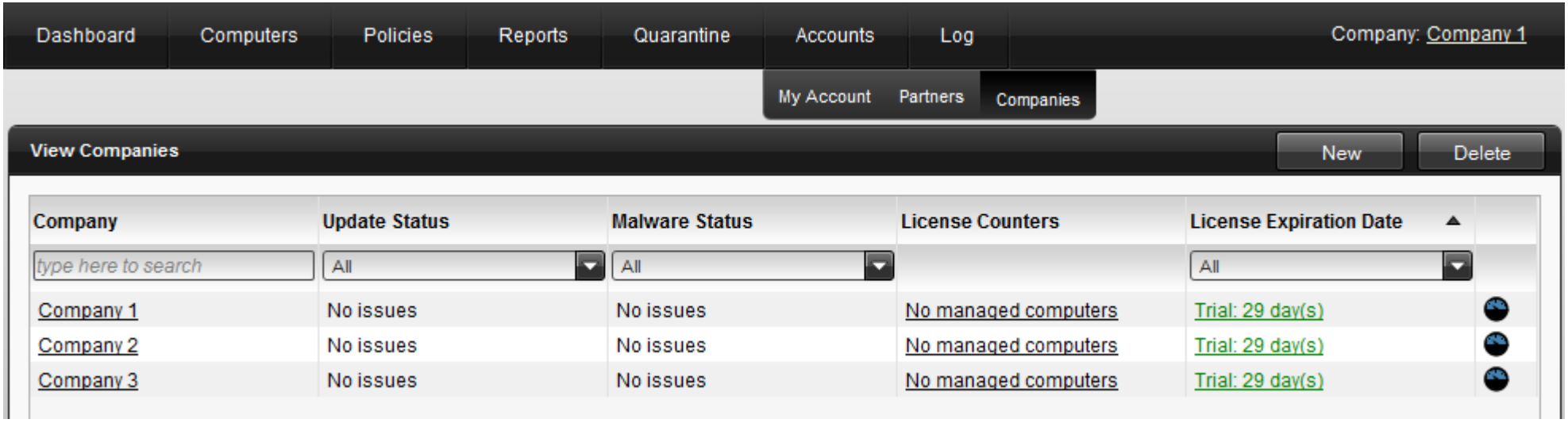
- Información de registro (caduca el..., no hay datos suficientes, evaluación)
- Imposibilidad para realizar las actualizaciones (se activa cuando un número determinado de clientes intentan actualizar y no consiguen hacerlo)
- Alerta de epidemia (para cada infección malware en un momento dado, se contabilizan los equipos infectados y estas notificaciones se muestran cuando se excede el número de máquinas infectadas)
- Políticas que no producen la eliminación de infecciones (para políticas configuradas para *aplicar la acción de* - rechazar cuando se encuentra un archivo infectado)
- Notificaciones personalizadas (disponibilidad de parches, periodo de mantenimiento, etc.)

Las notificaciones son información pura. No activan ninguna acción.

4.7 Organización de equipos

AÑADIR CLIENTES

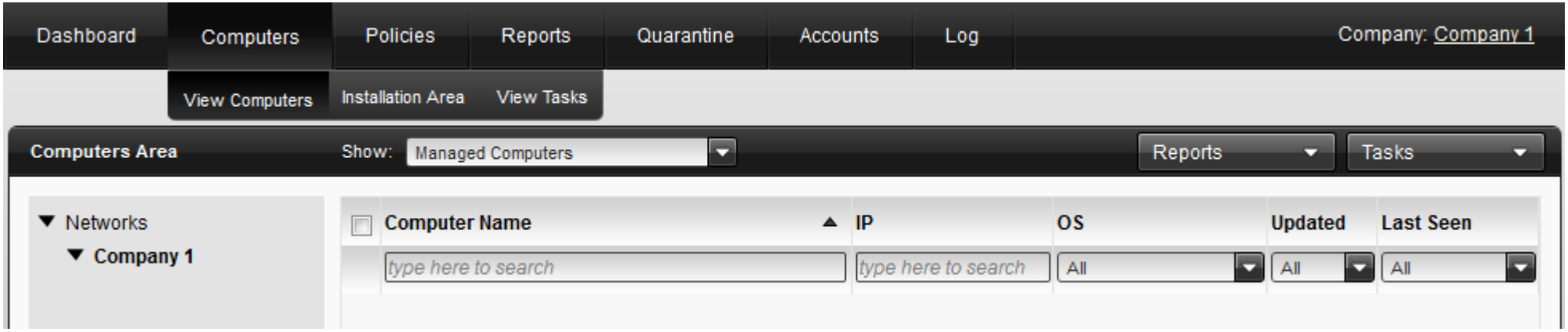
1. Un partner tiene que crear nuevos clientes (Empresas) **[Cuentas – Empresas – Nueva]**
2. Tan pronto como se crea la primera cuenta cliente (empresa) por un partner, el menú de la interfaz inicial cambia (se añaden nuevas pestañas y submenús)
3. Los Clientes/Empresas ahora se crean y visualizan en el área **[Cuentas – Empresas]**



4.7 Organización de equipos

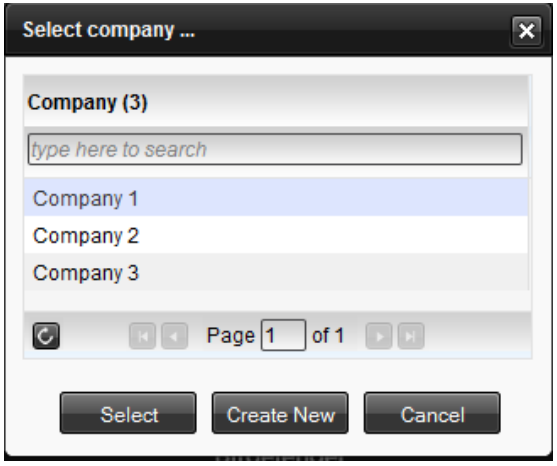
PREPARAR LA INSTALACIÓN

4. **[Equipos – Ver equipos]** también muestra las empresas creadas por el partner, pero en esta etapa los equipos clientes no se muestran, así que tenemos que acceder al Área de instalación y preparar la instalación de Endpoint Client.

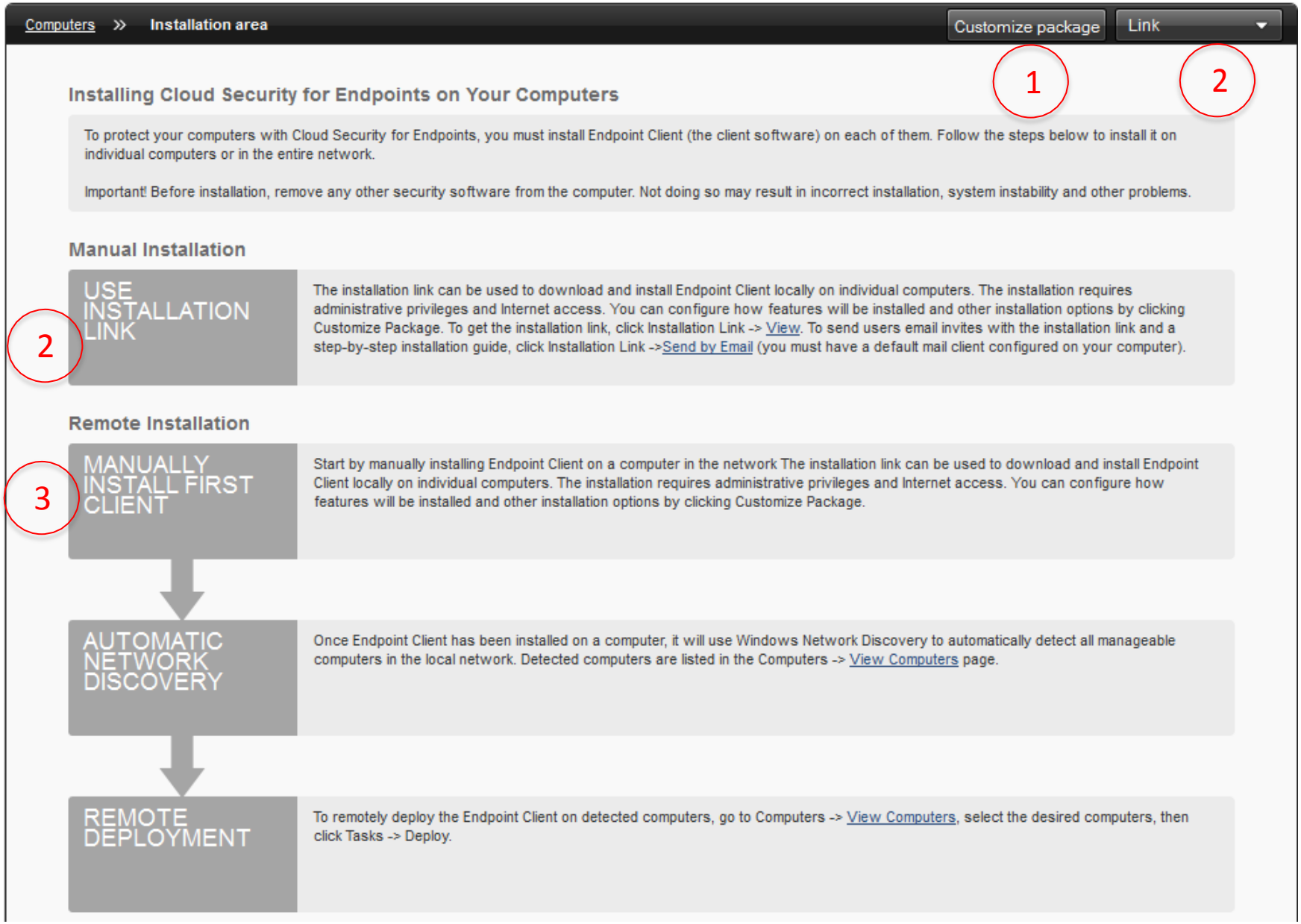


5. **[Equipos – Área de instalación]** Seleccione una red de la ventana emergente que se mostrará y encontrará los métodos de instalación:

- Instalación manual
- Instalación remota



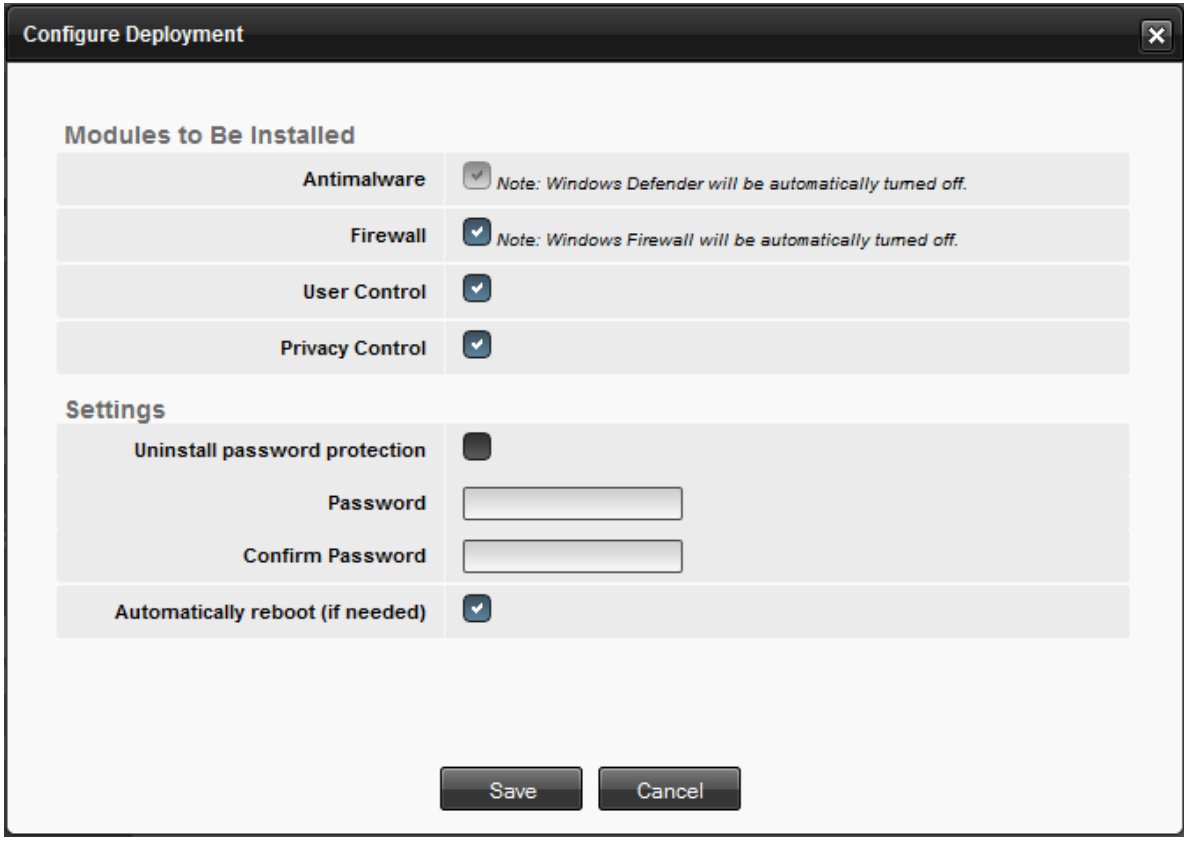
4.8 Organización de equipos – Área de instalación



4.8 Organización de equipos – Área de instalación

Personalizar paquete

1 La instalación requiere permisos de administrador y acceso a Internet. Podrá configurar los módulos que se instalarán y ajustar otras opciones haciendo clic en **[Personalizar paquete]**



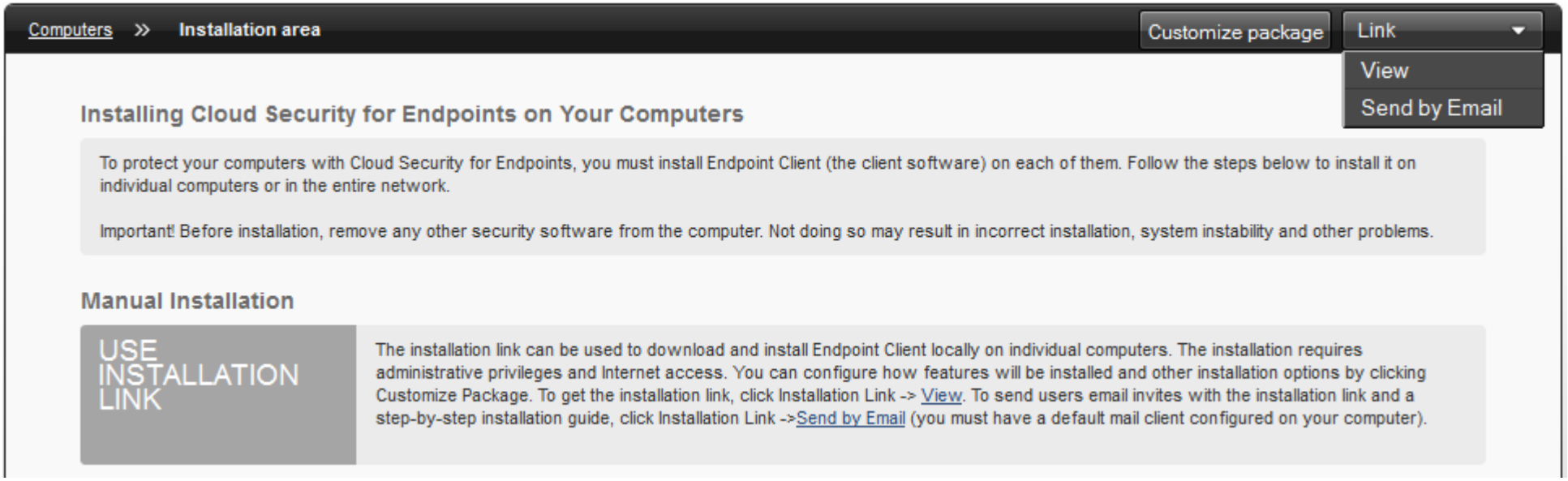
4.8 Organización de equipos – Área de instalación

2

Instalación manual (GUI en el emplazamiento del Endpoint)

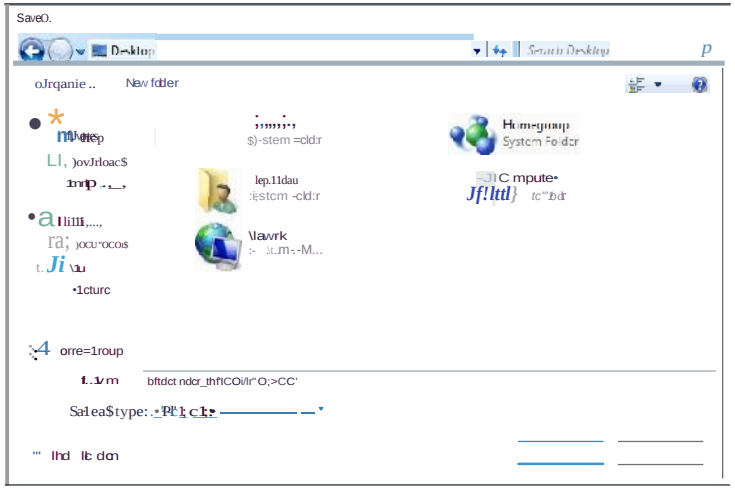
El enlace de instalación puede usarse para descargar e instalar el Endpoint Client localmente en equipos individuales.

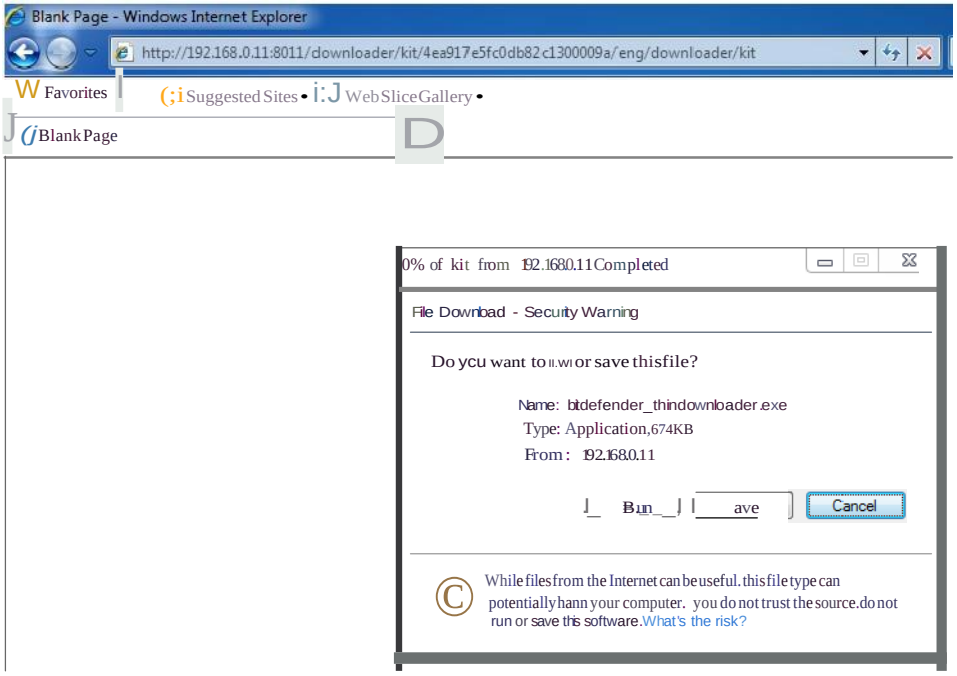
El **Enlace de instalación** le permitirá descargar un kit de instalación que puede copiarse a cualquier soporte para su uso posterior. Desde el menú desplegable Enlace puede elegir ver sólo el enlace o enviarlo por e-mail (puede enviarse por e-mail el enlace de descarga junto con una guía rápida de instalación)

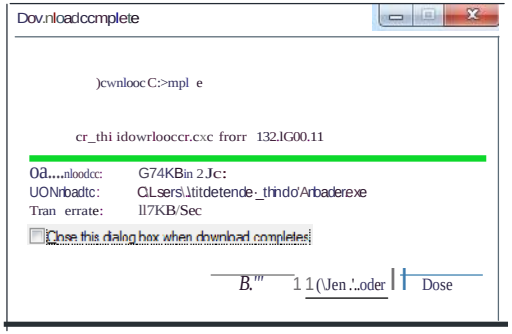


4.8 Organizaci6n de equipos – Area de instalaci6n

Bitdefender®







4.8 Organización de equipos – Área de instalación

ENDPOINT CLIENT - EQUIPO

Una vez descargado el kit desde el "enlace de instalación" podrá guardarlo en su equipo e iniciar la instalación. Este método de instalación no es silencioso, ya que el asistente de instalación le guiará a través de los distintos pasos de la instalación.

4.8 Organización de equipos – Área de instalación

ENDPOINT CLIENT - SERVIDOR

El mismo kit instalado en un servidor mostrará pasos de instalación ligeramente distintos que los que se muestran en una estación de trabajo. El paso de configuración indicará que solamente estará disponible el módulo Antimalware y obviamente la interfaz de Endpoint Client mostrará los módulos como "no instalados”.

4.8 Organización de equipos – Área de instalación

Instalación remota (sin GUI en el emplazamiento del Endpoint)

3

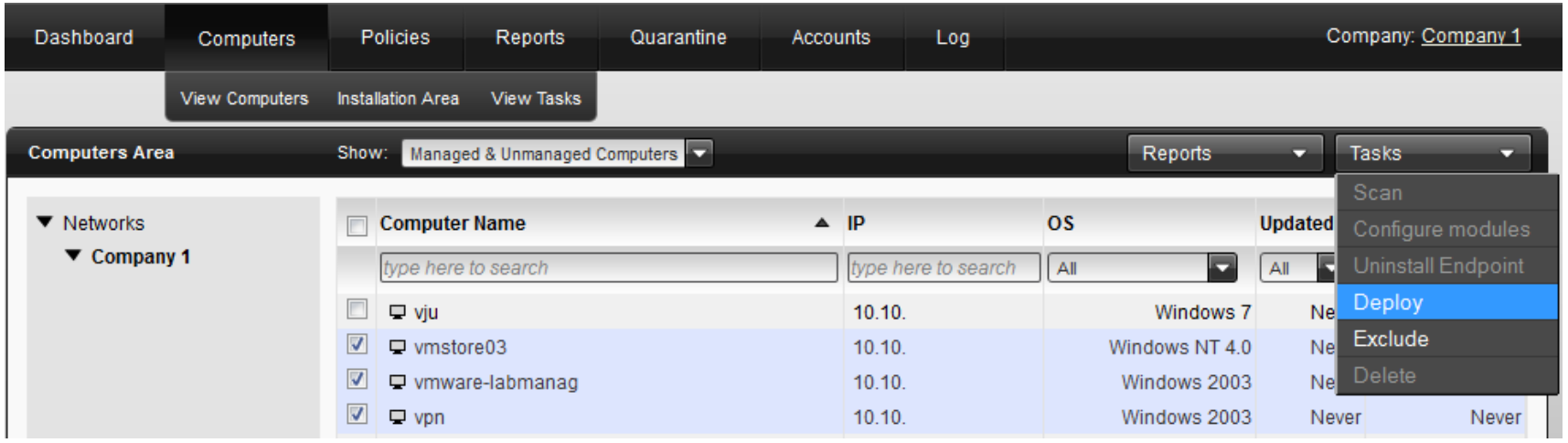
- Instalar manualmente primero el cliente – lo primero de todo sería instalar manualmente Endpoint Client en un equipo de la red. El enlace de instalación puede usarse para descargar e instalar Endpoint Client localmente en los equipos individuales.

- Descubrimiento automático de red

Una vez que Endpoint Client se ha instalado en un equipo, usará el Descubrimiento de Red de Windows para detectar automáticamente todos los equipos administrables en la red local.

- Instalación remota

Para instalar de forma remota el Endpoint Client en los equipos detectados, diríjase a **[Equipos – Ver equipos]**, seleccione los equipos deseados y luego, desde el menú **[Tareas]**, haga clic en **[Instalación].** El administrador tendrá que indicar las credenciales para todos los equipos seleccionados.



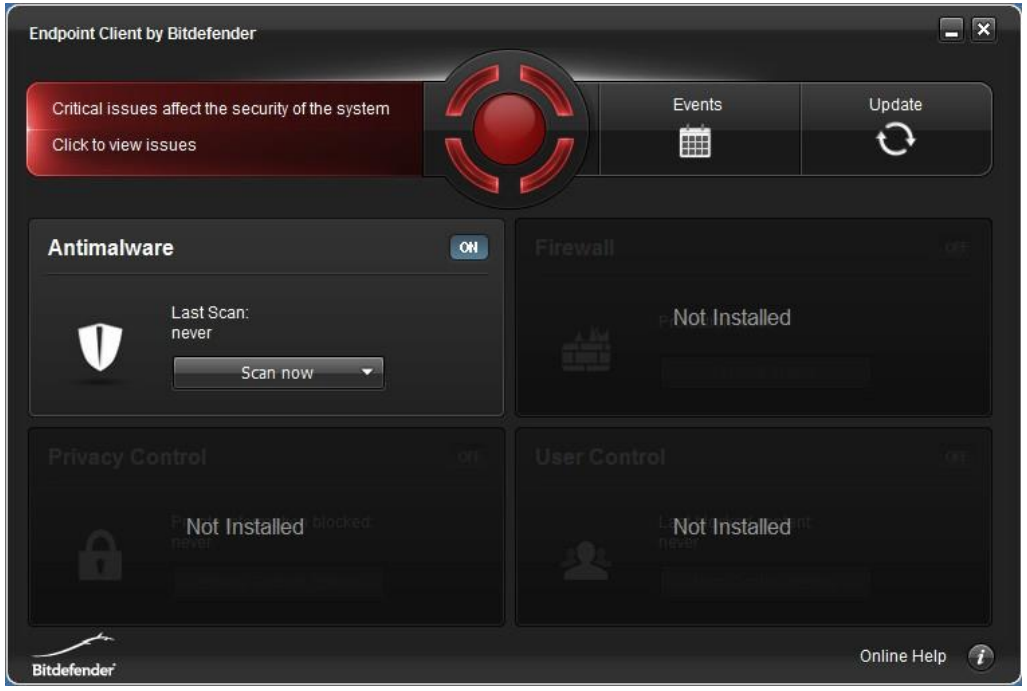
4.8 Organización de equipos – Área de instalación

DEL LADO DEL PUNTO FINAL, una vez completada la instalación:

Ligero. Bajo consumo de recursos del sistema.
Veloz. Análisis rápido y optimizado.
Silencioso. Discreto, con la mínima interacción del usuario.

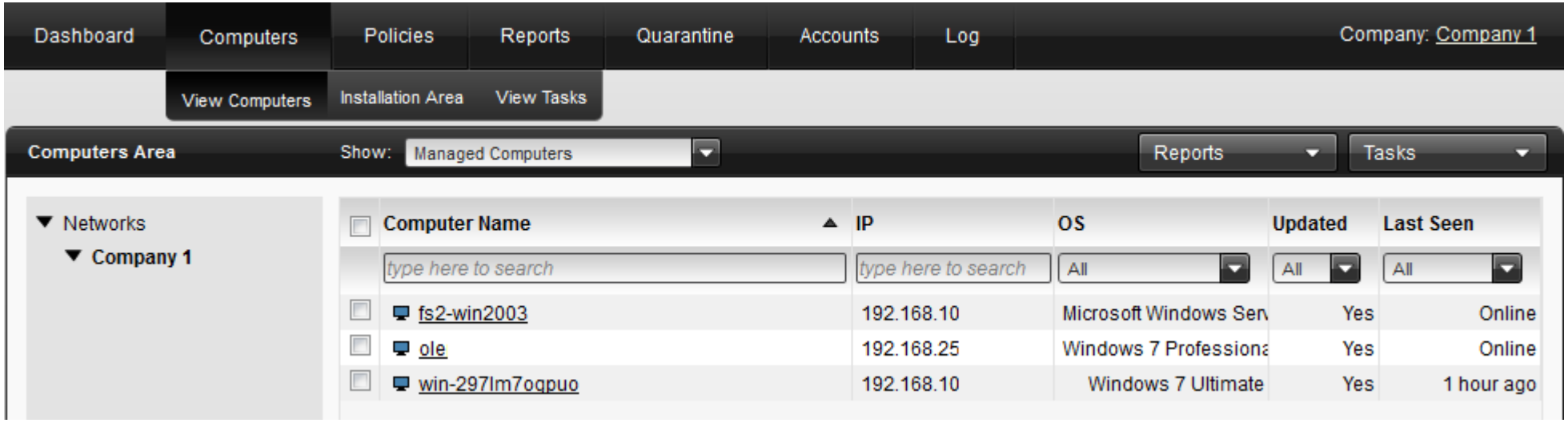
en EQUIPOS:

en los SERVIDORES:



4.9 Organización de equipos – Ver equipos

6. Una vez instalado el primer Endpoint Client en un equipo de su empresa, le ayudará a descubrir el resto de equipos de la red **[Equipos - Ver equipos]**. Configurando el filtro, puede mostrar los equipos administrables, no administrables, detectados y eliminados. También puede ejecutar los 8 informes disponibles **[Informes]** y realizar otras tareas **[Tareas]** seleccionando uno o varios equipos.



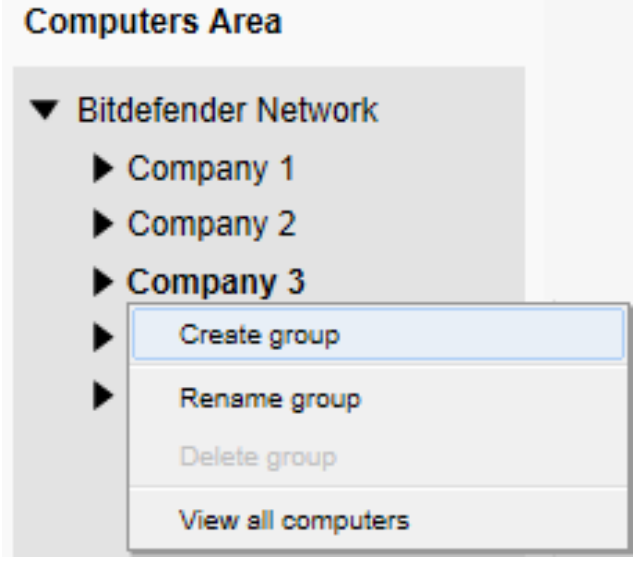
4.9 Organización de equipos – Ver equipos

Los **equipos no administrados** se representan mediante el icono  y no tienen una solución de seguridad (Endpoint Client) instalada.

Los **equipos administrados** están representados por el icono  y ya tienen instalado Endpoint Client, con lo que están protegidos por Bitdefender.

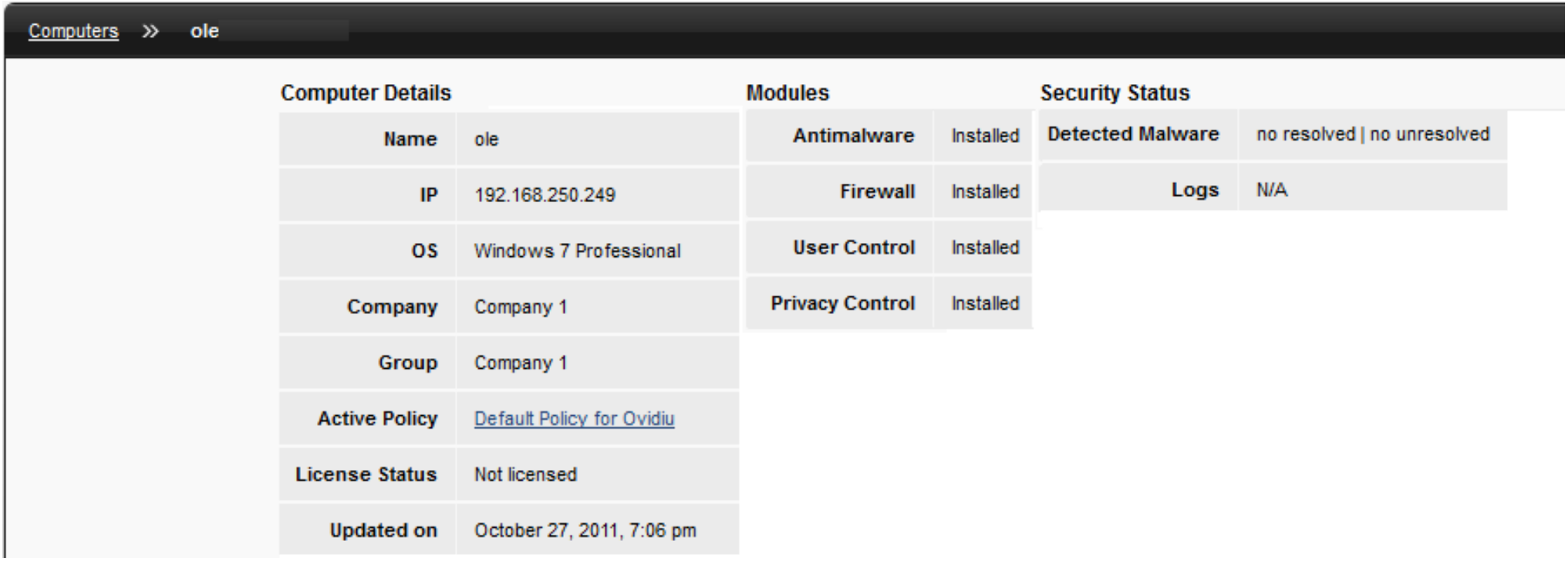
Los **equipos excluidos** están representados por el icono  , no son monitorizados de ninguna forma por Bitdefender y no son administrados.

Puede crear grupos para organizar los equipos dentro de la red.



4.9 Organización de equipos – Ver equipos

Al hacer clic en un equipo accede a los **Detalles del equipo** como: nombre, IP, SO, estado de licencia, política activa, malware solucionado o no solucionado. También podrá comprobar el estado de los módulos: instalado, no instalado, activo, inactivo y ver el registro del último análisis.



4.10 Endpoint Client – Configuración de usuario y paneles

Bitdefender Endpoint Client protege las estaciones de trabajo de la empresa y se administra desde la nube a través de Bitdefender Security Console.

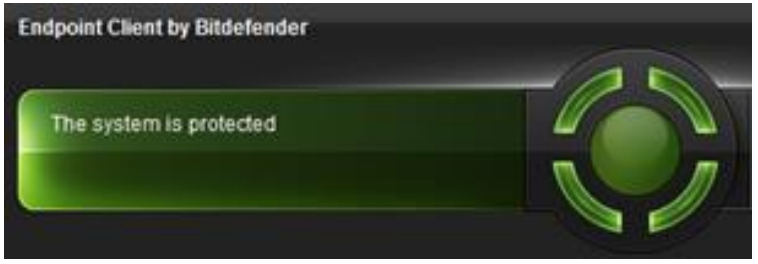
Endpoint Client de Bitdefender está configurado y administrado de forma remota por su administrador de red o Proveedor de servicios. No puede cambiar las opciones de protección. Si tiene alguna pregunta relativa a sus ajustes de protección, por favor, envíelas a la persona responsable de la seguridad de su red.

Una vez que se haya instalado Bitdefender Endpoint Client, su equipo estará protegido contra todo tipo de amenazas (malware, spam, hackers, contenido inapropiado, etc.).

Sólo podrá:

- Ver cualquier incidencia que afecte a la seguridad del sistema (según el área de estado de seguridad en el lateral izquierdo de la barra de herramientas) – **3 posibles estados**:

VERDE – El sistema está protegido (no hay incidencias)



4.10 Endpoint Client – Configuración de usuario y paneles

ROJO - Incidencias críticas afectan a la seguridad del sistema

- El producto no está sincronizado con el servidor.
- Protección en tiempo real está desactivada.
- Analizar todos los archivos o sólo aplicaciones está desactivado.
- No se ha realizado un análisis de sistema en los últimos x días.
- El cortafuego está desactivado.
- Antiphishing está desactivado.
- El producto no está actualizado.
- Necesita reiniciar el PC para completar la actualización.

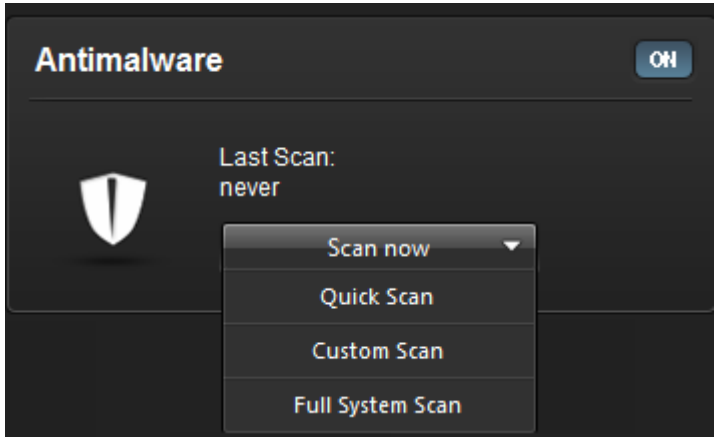
NARANJA - Algunas incidencias afectan la seguridad del sistema

- Es necesario reiniciar para realizar una operación de restauración de la cuarentena.
- Hay que reiniciar para completar la operación de mantenimiento.
- La protección de datos está desactivada.
- El control de usuario está desactivado.

4.10 Endpoint Client – Configuración de usuario y paneles

- Vea el historial de eventos (para los distintos módulos disponibles). Para los servidores sólo se muestran eventos antimalware, de actualización y varios.

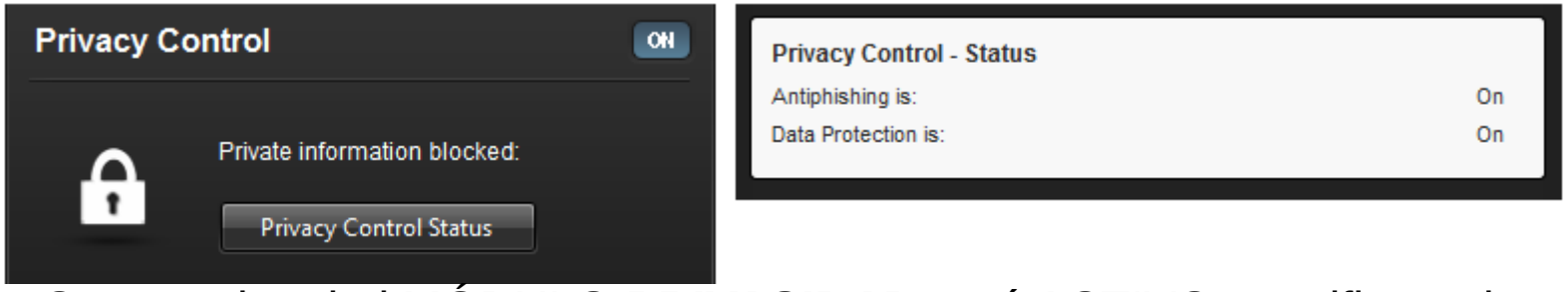
- Ver el estado de actualización, la última comprobación de actualización y realizar una actualización.



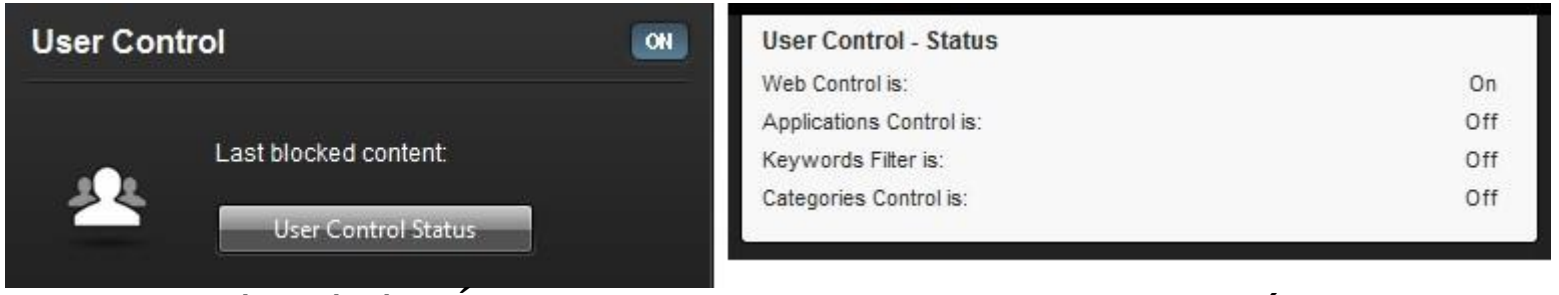
- Compruebe si el MÓDULO **ANTIMALWARE** está ACTIVO y realice un análisis del sistema rápido, completo o personalizado.

4.10 Endpoint Client – Configuración de usuario y paneles

- Compruebe si el MÓDULO **CORTAFUEGO** está ACTIVO y verifique su estado ***(sólo para estaciones de trabajo)***



- Compruebe si el MÓDULO **PRIVACIDAD** está ACTIVO y verifique el estado ***(sólo para estaciones de trabajo)***



- Compruebe si el MÓDULO **CONTROL DE USUARIO** está ACTIVO y verifique su estado ***(sólo para estaciones de trabajo)***

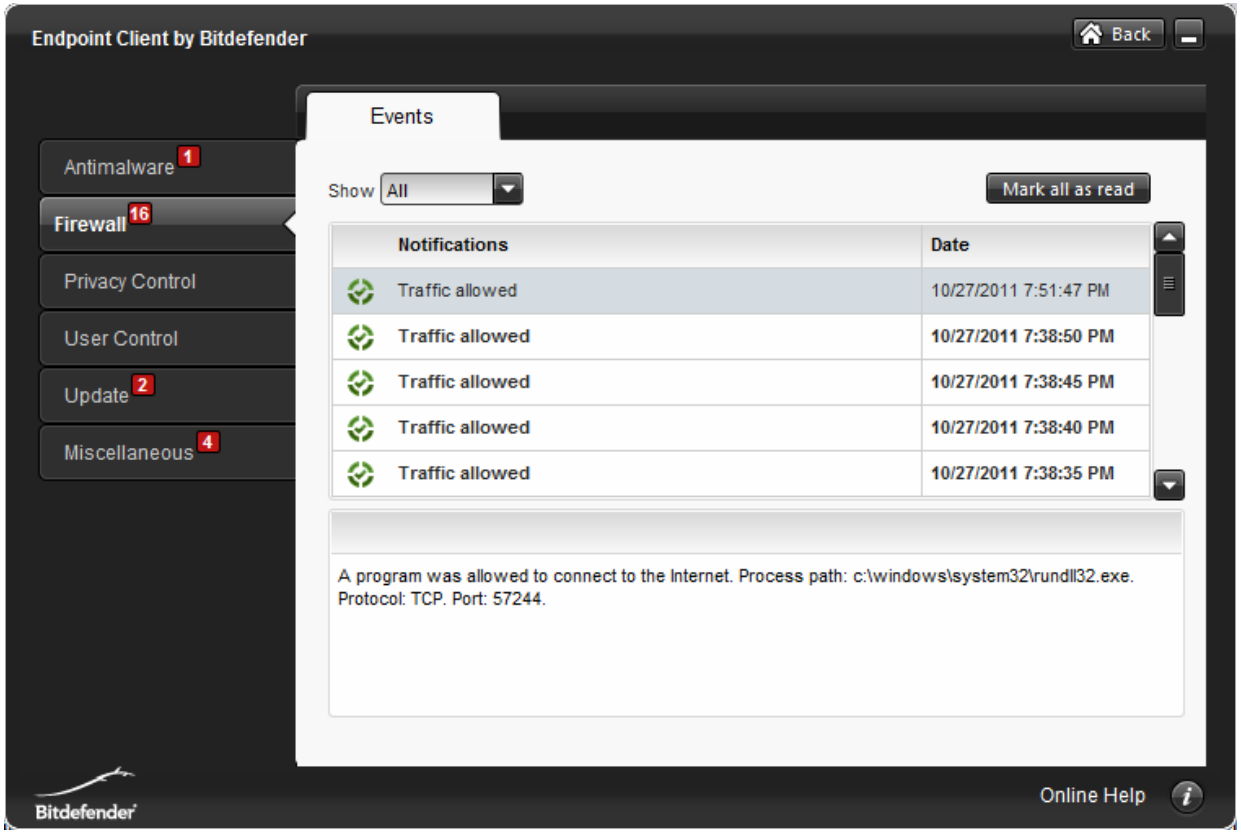
4.10 Endpoint Client – Configuración de usuario y paneles

4.11 ndpoint Client – Eventos

Endpoint Client de Bitdefender mantiene un registro detallado de los eventos asociados con su actividad en su equipo (incluyendo también las actividades del equipo monitorizadas por el Control de usuario). Los eventos son una herramienta muy importante en la monitorización de la protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontró malware en su equipo, etc.

Seleccione la categoría de evento en el menú izquierdo. Los eventos se agrupan en las siguientes categorías:

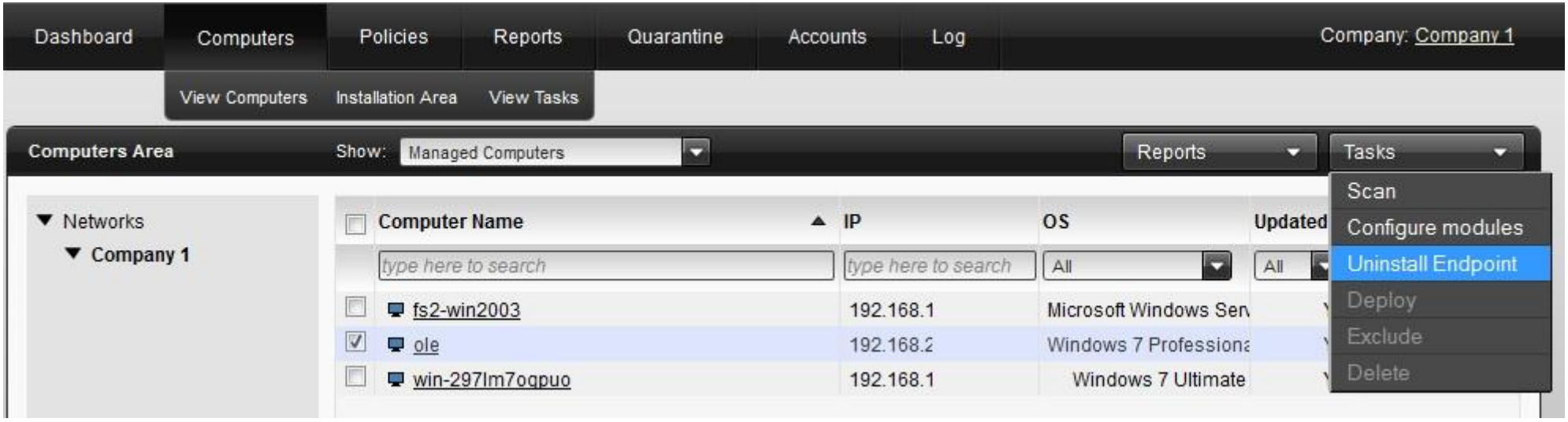
Antimalware
Actualizaciones
Control de privacidad
Cortafuego
Varios
Control de usuario



4.12 Endpoint Client – Desinstalar

DESDE CLOUD SECURITY CONSOLE:

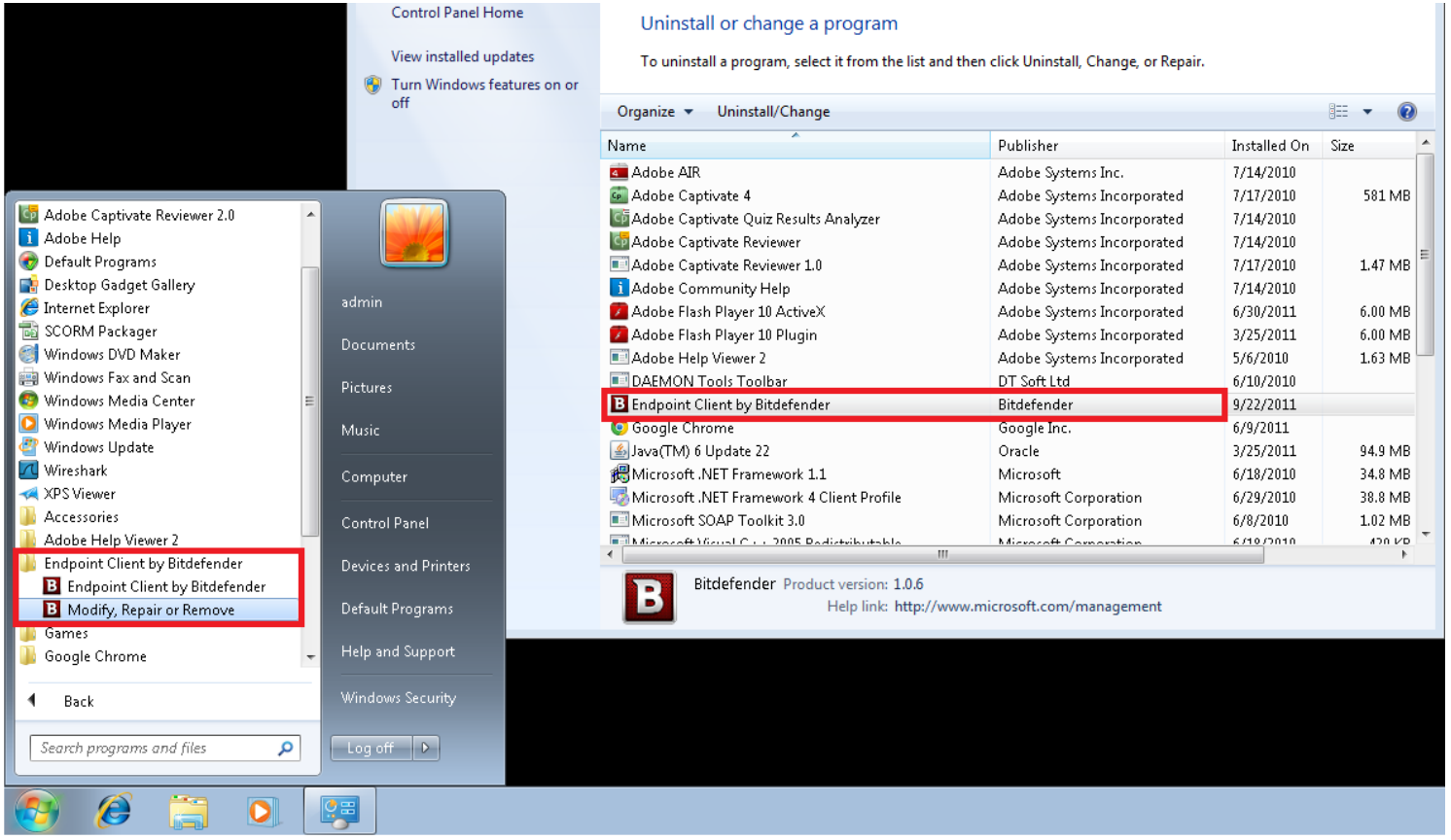
Para desinstalar Endpoint Client, puede ir a **[Equipos, Ver equipos]**, marcar los equipos en los que quiere desinstalar Endpoint Client y, desde la lista desplegable **[Tareas]**, seleccionar **[Desinstalar Endpoint].** Esto comenzará un proceso de desinstalación silencioso sin ninguna interfaz de usuario.



4.12 Endpoint Client – Desinstalar

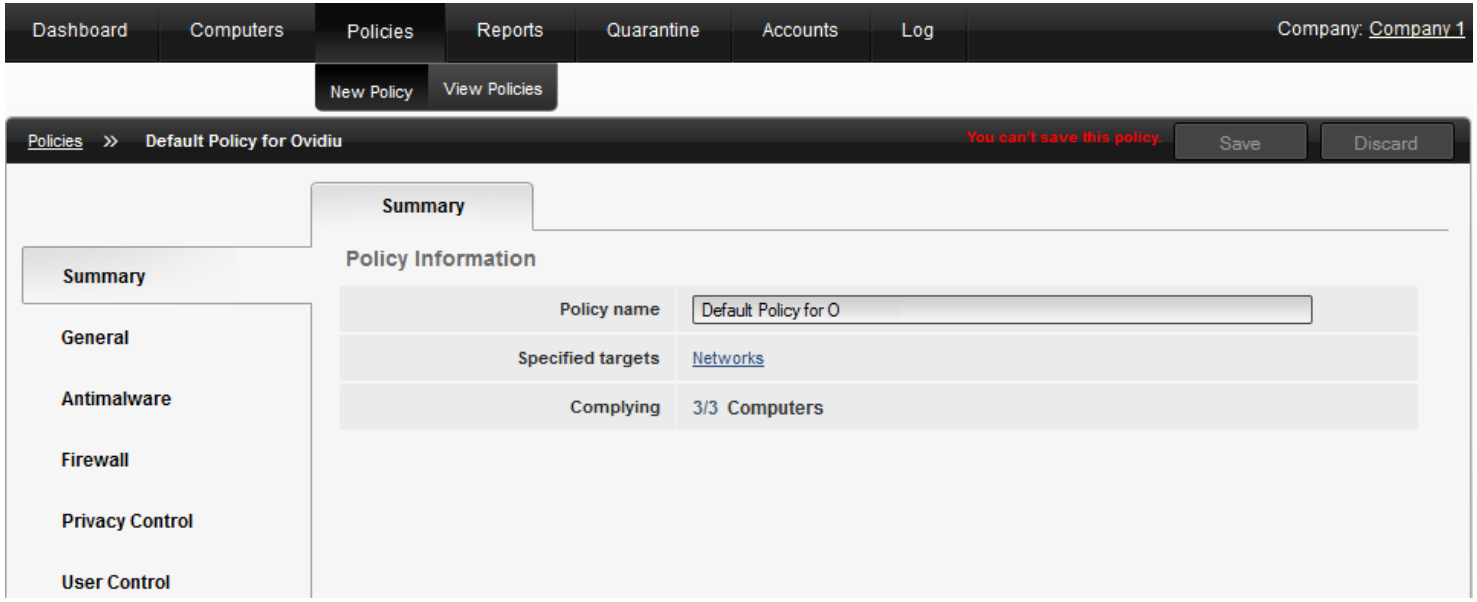
DESDE EL ENDPOINT CLIENT:

Para desinstalar el Endpoint Client, puede realizar esta acción bien desde **Windows – Menú Inicio**, o desde el **Panel de control, Programas**. Esto iniciará un asistente de desinstalación con GUI.



4.13 Políticas

- Una plantilla de política predeterminada para configurar todos los módulos. La plantilla de política contiene 5 módulos con varias pestañas por módulo y le permite configurar al detalle las políticas que creará.



- La política se aplica solamente a los módulos detectados.
- La política es efectiva cuando se envía y aplica.
- Pueden aplicarse varias políticas al mismo tiempo, en los mismos equipos objetivo, pero la última política creada siempre se aplica.
- Siempre existirá una única política activa.
- No es necesaria sincronización. Las políticas se "aplican" siempre.

4.13 Políticas – Visión general de la plantilla predeterminada

Resumen

(nombre de política, objetivos especificados, cumplimiento)

General

Mostrar (administración de notificaciones y opciones on-off de las alertas del estado de módulos)
Avanzado (configuración y protección por contraseña)
Actualización (configuración de las opciones de actualización)

Antimalware

On-access (o protección en tiempo real - configuración de ajustes más configuración de AV)
Bajo demanda (administración de tareas de análisis)
Exclusiones (activación y configuración de las exclusiones de análisis)
Cuarentena (configuración de cuarentena)

Cortafuego

Configuración (configuración del cortafuego y del sistema de detección de intrusiones)
Perfiles (perfiles por tipo de red o adaptador)
Avanzado (reglas de cortafuego: añadir, editar, cambiar permisos)

4.13 Políticas – Descripción de la plantilla predeterminada

Control de privacidad

Antiphishing (opciones de la barra de herramientas, asesor de búsquedas, protección para el navegador Web, administración de la lista blanca)

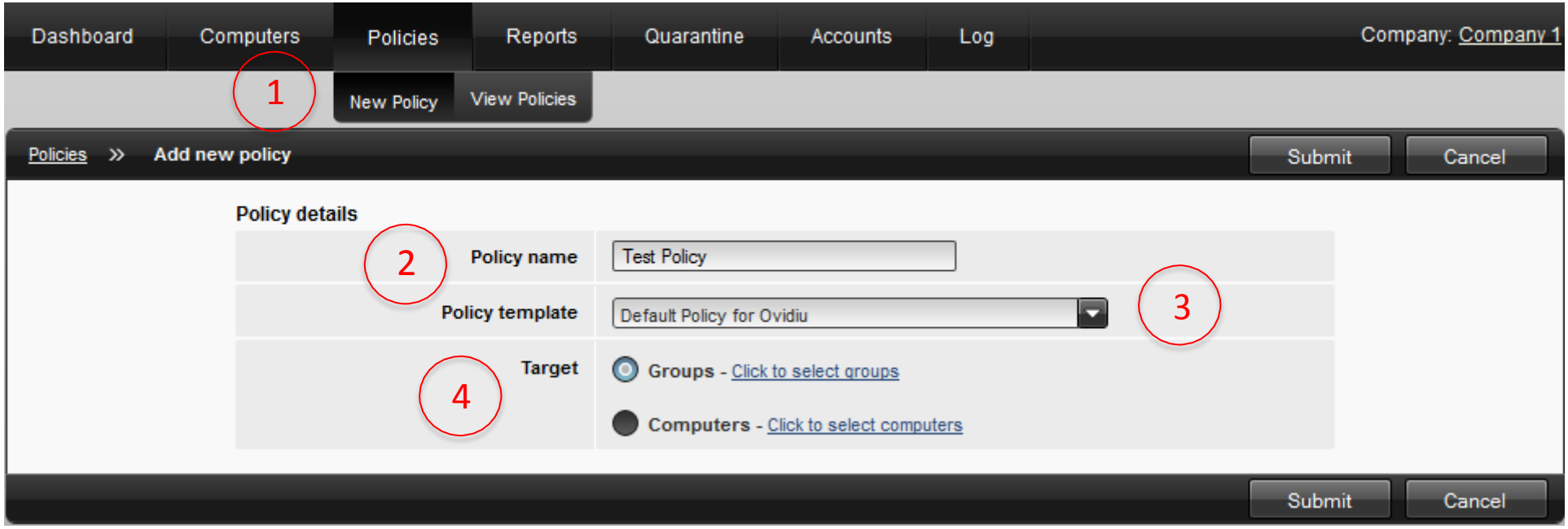
Lista blanca (añadir sitios Web)

Control de usuario

General (facilita activar o desactivar los módulos listados debajo y permite bloquear o programar el acceso Web)
Control Web (administra las reglas Web añadiéndolas, eliminándolas, programándolas o cambiando los permisos)

Control de categorías (los permisos cambian para el perfil de categoría, y permite configurar permisos o restricciones para una lista de categorías predefinidas tales como bloqueador proxy Web, noticias, etc.)

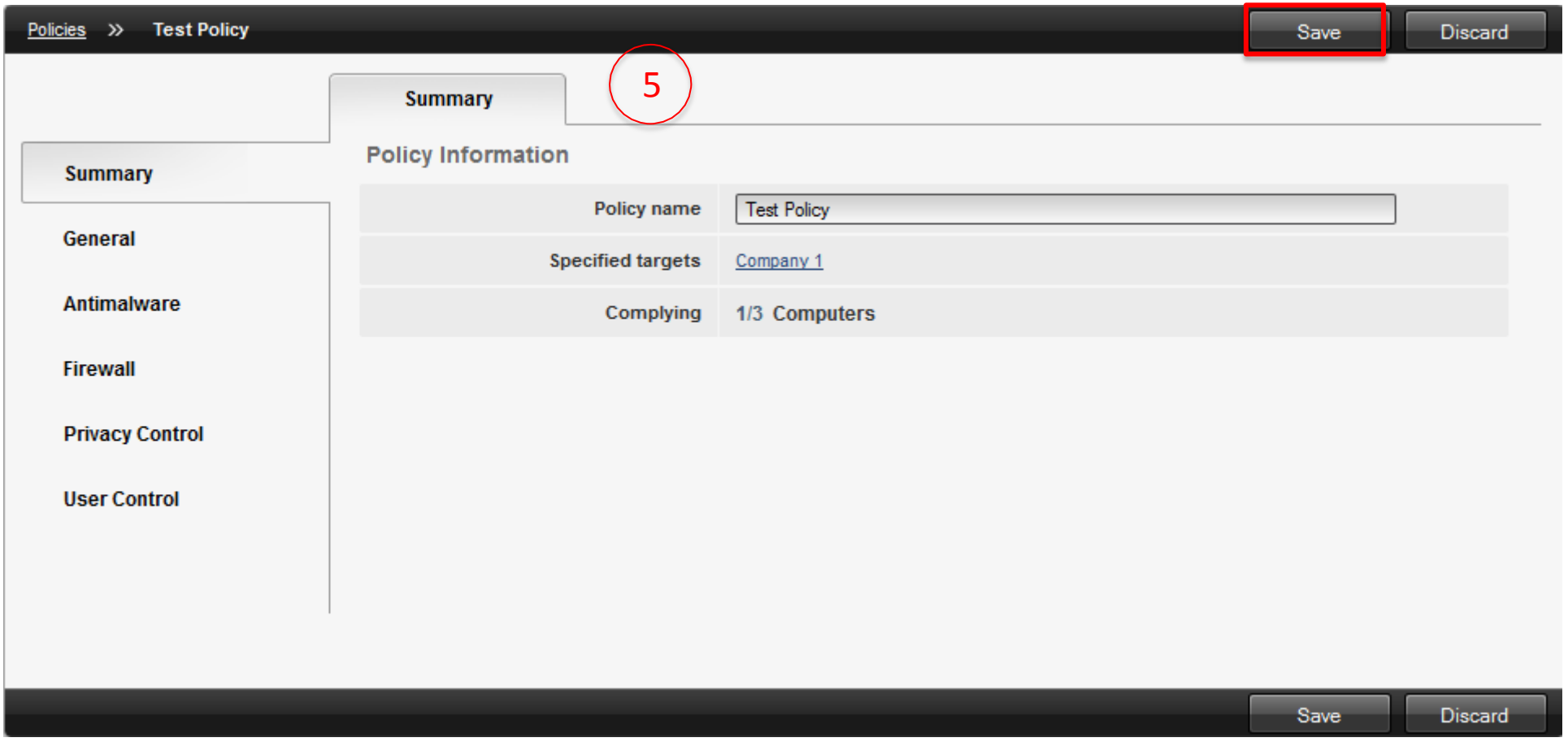
4.13 Políticas – Crear y aplicar políticas



1. Políticas – Nueva política
2. Escriba el nombre de la política
3. Seleccione la plantilla de política que desea usar. Puede usar una plantilla creada anteriormente sólo para editarla.
4. Seleccione un grupo de equipos o un equipo al que desea enviar la política

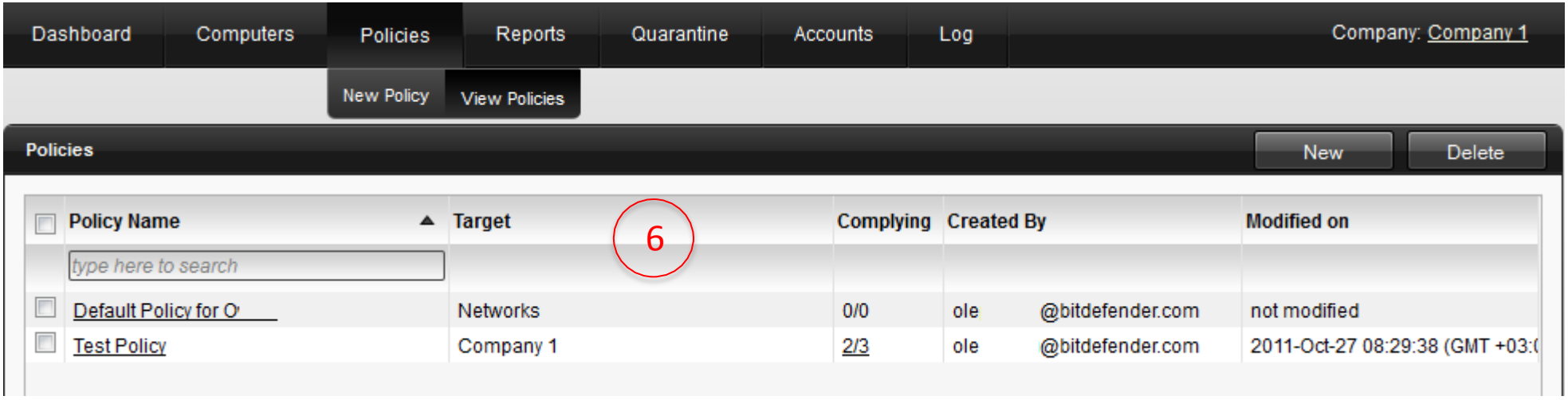
4.13 Políticas – Crear y aplicar políticas

5. Se mostrará la plantilla de política. Aquí puede configurar las opciones de la política por módulos. Una vez configurada la política, puede guardarla.



4.13 Políticas – Crear y aplicar políticas

6. Una vez guardada la política, se listará en el menú "Ver políticas". El cumplimiento indicará si la política se aplicó en los equipos seleccionados. 0/1 significa que la política se envió a un equipo y 1/1 significa que la política se aplicó en el equipo al que se envió.



Tan pronto como se haya completado el cumplimiento, podrán comprobarse los resultados de la política aplicada en el Endpoint Client.

4.14 Informes

Bitdefender Cloud Security for Endpoints le permite crear y visualizar informes centralizados sobre el estado de seguridad de los equipos administrados.

Todos los informes generados están disponibles en la consola Bitdefender Cloud Security for Endpoints durante un periodo predeterminado de 30 días, pero puede guardarlos en su equipo o enviarlos por correo. Los formatos disponibles incluyen Portable Document Format (PDF) y valores separados por comas (CSV).

Los informes pueden usarse para múltiples propósitos, tales como:

- Monitorizar y asegurar el cumplimiento con las políticas de seguridad de la organización.
- Comprobar y evaluar el estado de seguridad de la red.
- Identificar incidencias de seguridad de la red, amenazas y vulnerabilidades.
- Monitorizar los incidentes de seguridad y la actividad malware.
- Proporcionar una administración superior con datos de fácil interpretación sobre la seguridad de la red..

4.14 Informes

9 tipos de informe disponibles (6 informes accesibles desde el Panel de control + 3 informes sólo disponibles desde la sección Informes)

Los informes pueden consolidar información de toda la red de equipos administrados o de grupos específicos solamente. De esta forma, desde un sólo informe, puede descubrir:
- Datos estadísticos relativos a todos los equipos o los grupos administrados.
- Información detallada para cada equipo administrado.
- La lista de equipos que cumplen un criterio específico (por ejemplo, aquellos que tienen desactivada la protección antimalware).

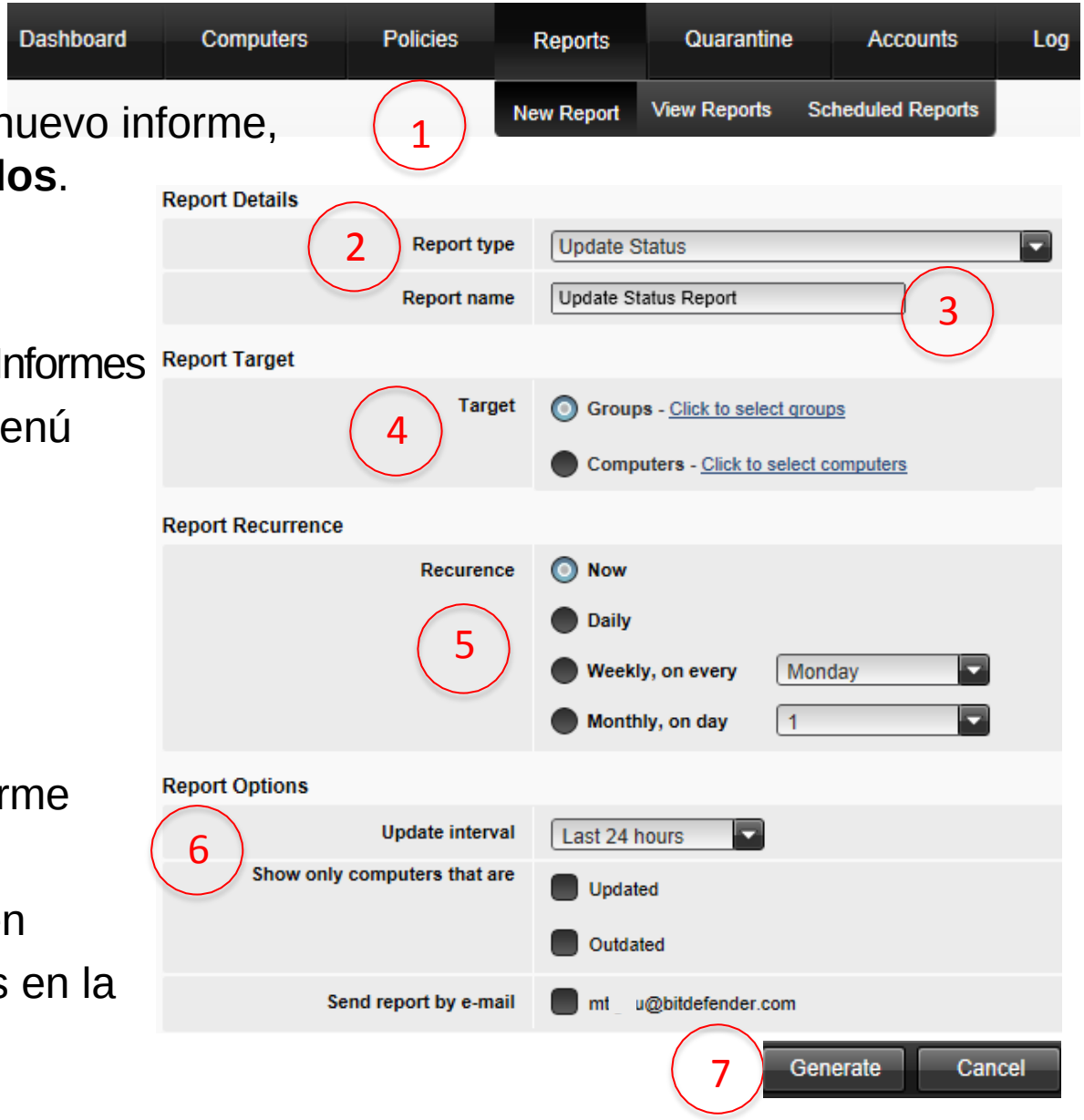
4.14 Informes – Crear informes

Desde la **sección** informes puede **crear** un nuevo informe, **ver** informes creados e informes **programados**.

Crear un nuevo informe:

1. Seleccione "Nuevo informe" desde la sección Informes
2. Seleccione el tipo de informe desde el menú
3. Indroduzca un nombre descriptivo
4. Configure el objetivo del informe
5. Establecezca la periodicidad del informe (ahora o programado)
6. Establezca las opciones del informe
7. Haga clic en "Generar" para crear el informe

Verá los informes creados inmediatamente en la sección "**Ver informes**" y los programados en la sección "**Informes programados**".



4.14 Informes – Ver informes

Para ver y administrar los informes generados, diríjase a la página **Informes** > **Ver informes**. Esta página se muestra automáticamente tras crear un informe inmediato (los informes programados pueden administrarse en la página Informes > Informes programados).

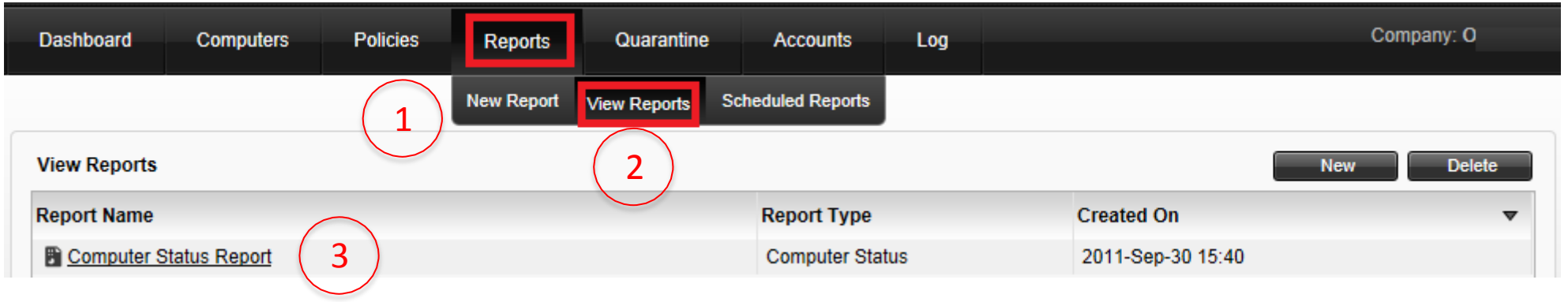
Puede ver los informes generados e información útil acerca de ellos:

- El nombre y tipo del informe.
- Cuándo se generó el informe.

Cada informe se marca con uno de los siguientes iconos para indicarle si el informe está programado o no:

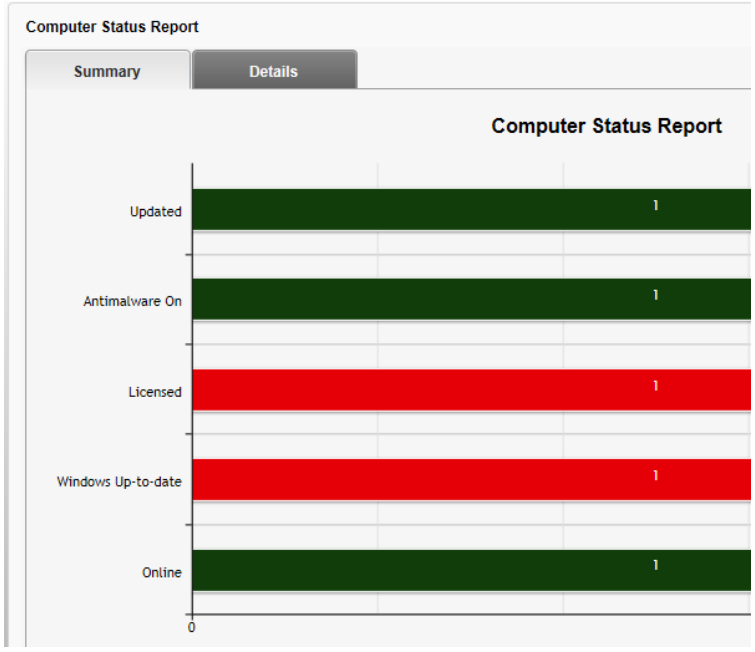
Update Status Report indica un informe programado.

Update Status Report indica un informe normal.

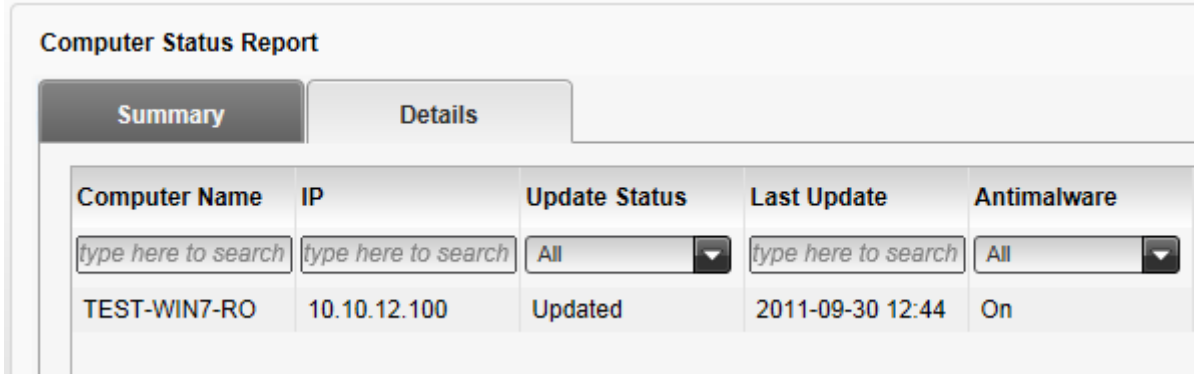


4.14 Informes – Ver informes

Haga clic en el nombre del informe que desea ver. Para encontrar rápidamente el informe que está buscando puede ordenar los informes por nombre, tipo u hora de creación.



La página **Resumen** le proporciona datos estadísticos (gráficos de tarta y diagramas) para todos los equipos objetivo o grupos.



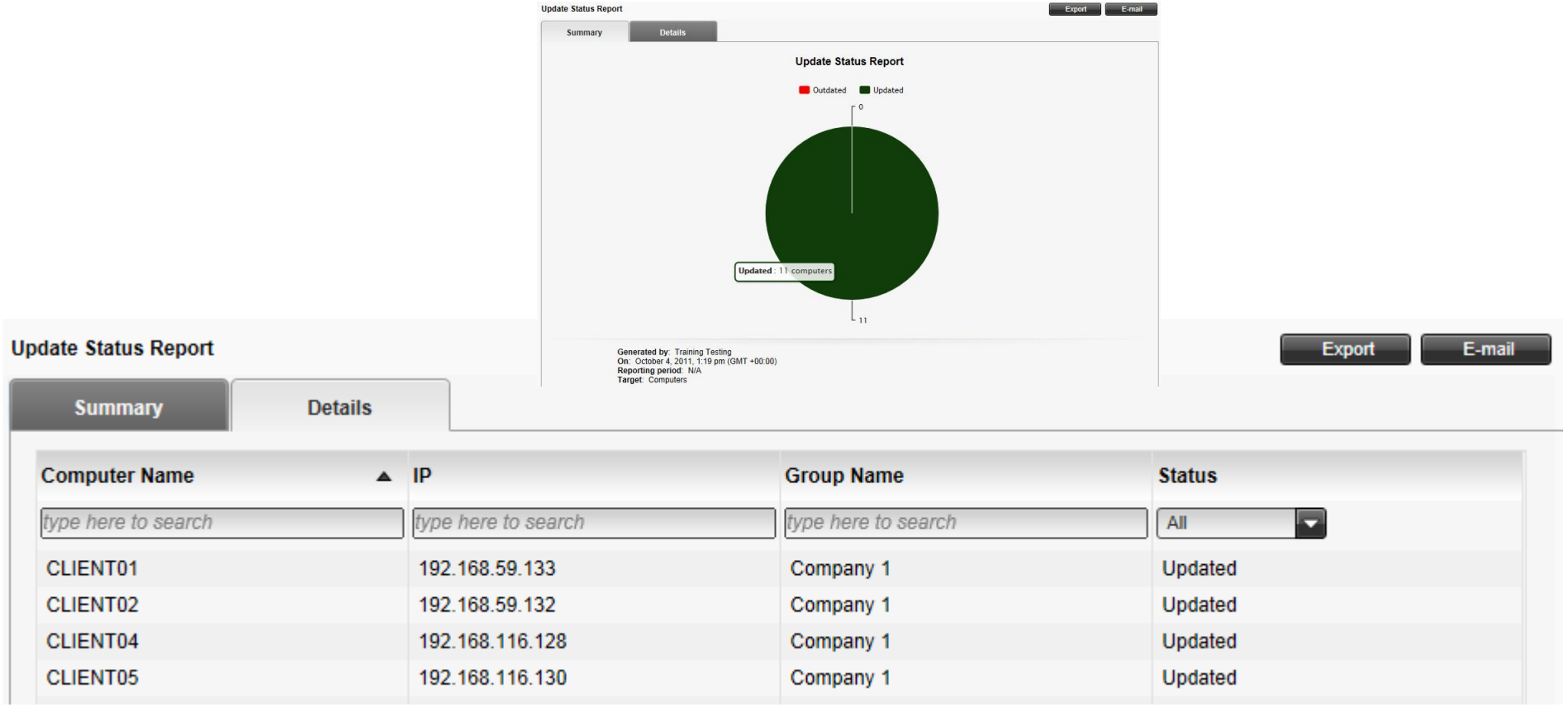
La página **Detalles** proporciona información en detalle para cada equipo administrado.

- Nombre del equipo
- IP
- Estado de actualización
- Ultima actualización
- Antimalware
- Estado de licencia
- Estado de Windows Update
- Online

4.14 Informes – Estado de actualización

ESTADO DE ACTUALIZACIÓN

Le muestra el estado de actualización de la protección Bitdefender Cloud Security for Endpoints instalada en los equipos seleccionados. Utilizando los filtros disponibles, puede descubrir fácilmente qué clientes se han actualizado o no en un periodo de tiempo específico.

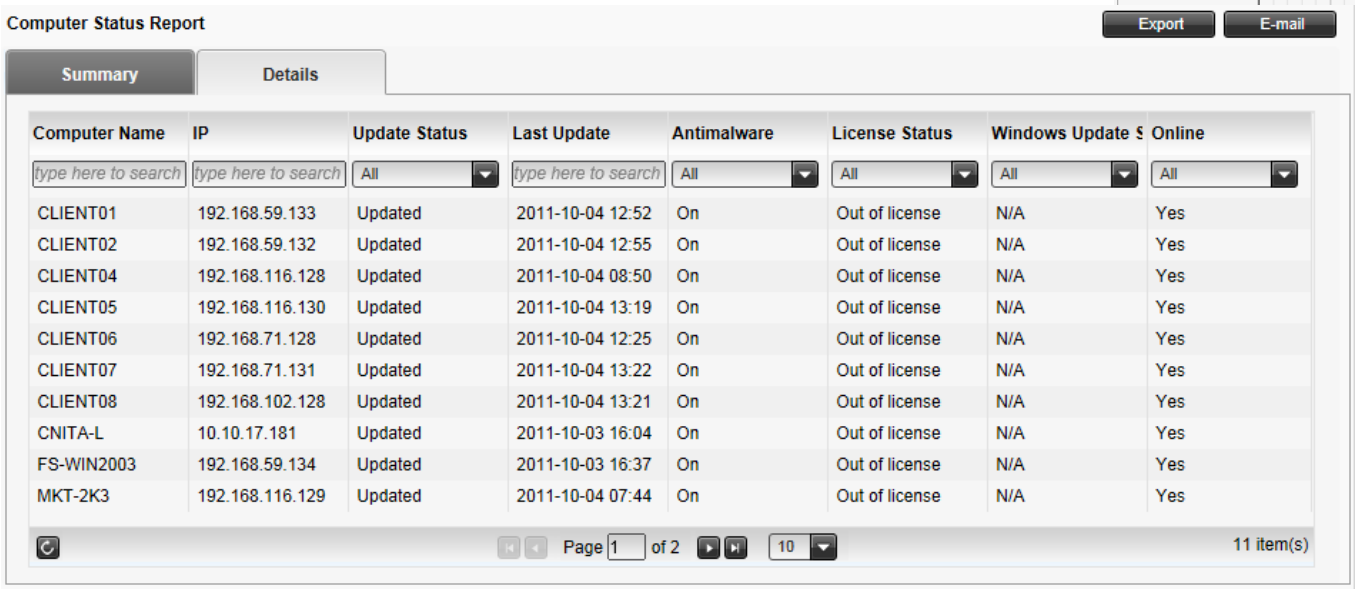


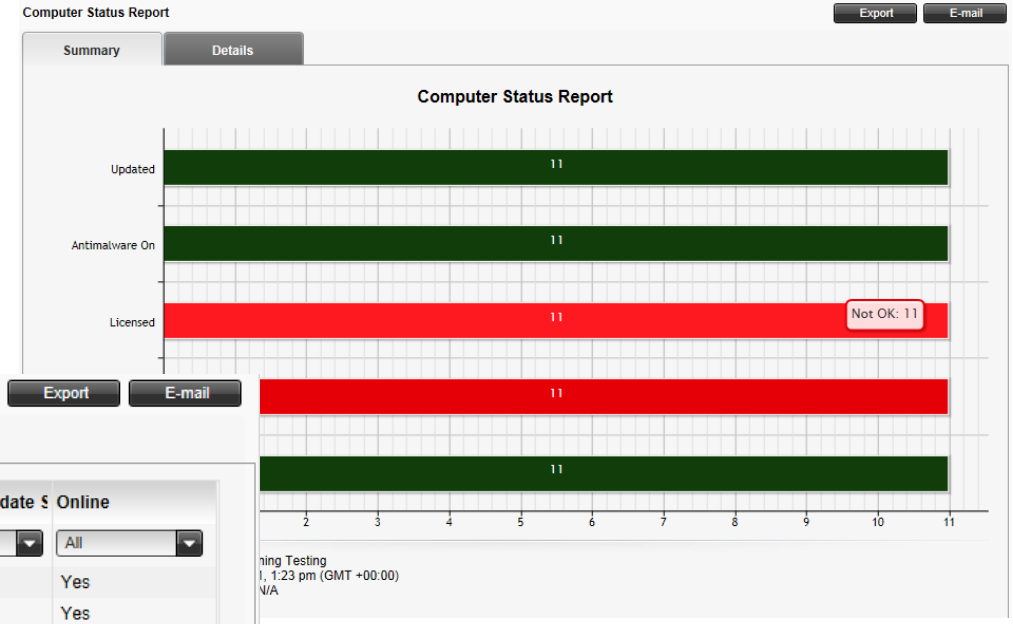
4.14 Informes – Estado del equipo

ESTADO DEL EQUIPO

Le proporciona diversas informaciones de estado relativas a los equipos seleccionados en los que se ha instalado la protección Bitdefender Cloud Security for Endpoints.

- Estado de actualización de la protección
- Estado de licencia
- Estado de actividad de la red (online/offline)
- Estado de protección antimalware
- Estado de actualización de Windows

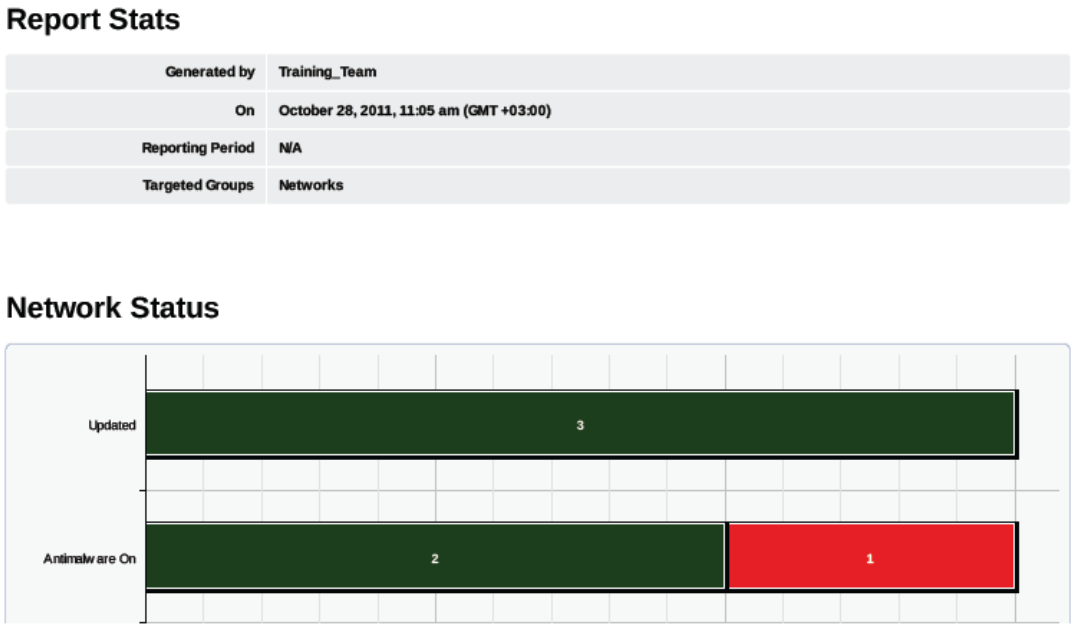




4.14 Informes – Ejecutivo

INFORME EJECUTIVO

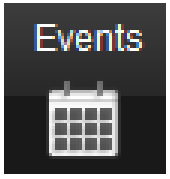
Este informe le permite exportar un archivo ZIP que contiene un documento PDF que presenta los 6 portlets del panel de control (diagramas gráficos exportados desde el panel de control).

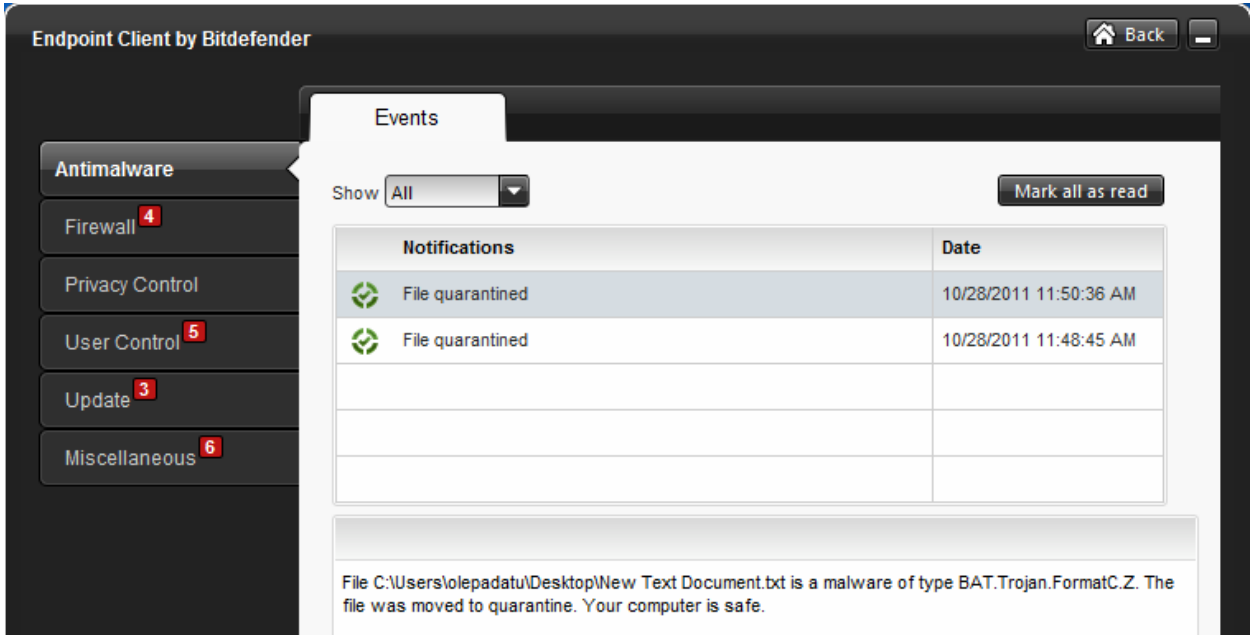


4.15 Cuarentena

El software cliente Bitdefender Cloud Security for Endpoints aísla los archivos sospechosos y los archivos infectados con malware que no puede desinfectar en un área segura denominada cuarentena. Cuando un virus está en la cuarentena no puede causar ningún daño porque no puede ni ejecutarse ni ser leído.
Cada cliente posee su propia carpeta de cuarentena. Los archivos de cuarentena se envían de forma predeterminada y automáticamente a los laboratorios de Bitdefender para ser analizados por los investigadores de malware de Bitdefender. Si se confirmase la presencia de malware se publicará una firma que permita eliminar dicho malware.

EN EL ENDPOINT CLIENT



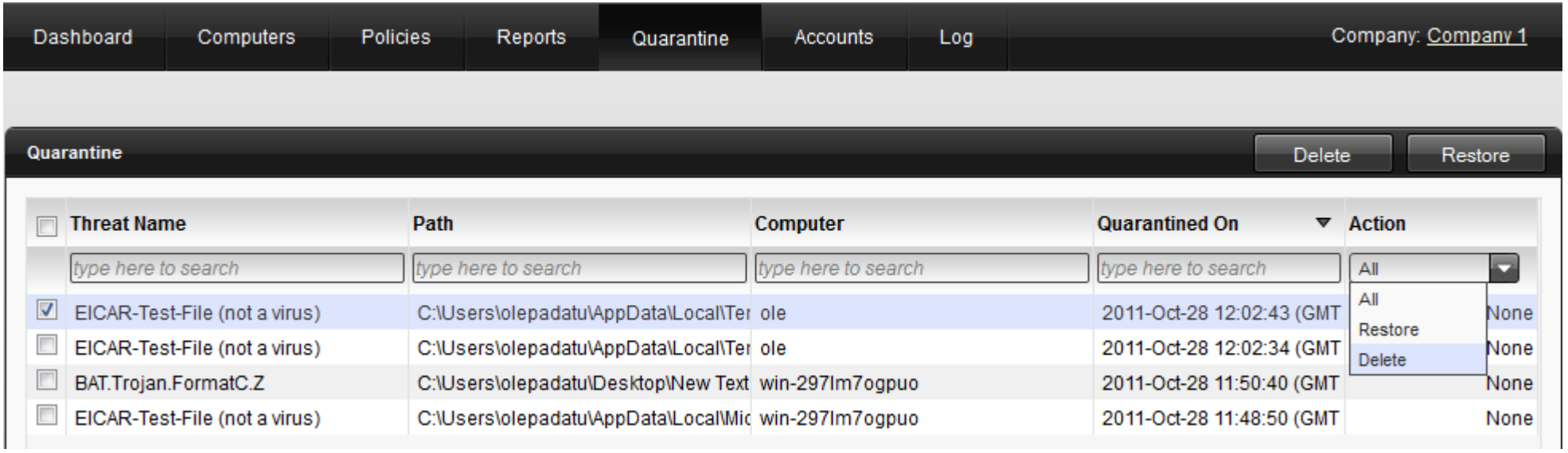


4.15 Cuarentena

Además, los archivos en cuarentena se analizan tras cada actualización de firmas malware. Los archivos limpiados se trasladan automáticamente a sus ubicaciones originales.

EN CLOUD SECURITY CONSOLE

Bitdefender Cloud Security for Endpoints proporciona información detallada sobre todos los archivos trasladados a la cuarentena en los equipos administrados desde su cuenta.



4.15 Cuarentena

Administración de los archivos en cuarentena

En determinadas ocasiones, puede que necesite restaurar archivos de la cuarentena, bien sea a su ubicación original o a otra alternativa. Una de estas situaciones se produce cuando quiere recuperar datos importantes almacenados en un archivo infectado que ha sido incluido en la cuarentena. Podrá elegir la ubicación donde quiere que se restauren los archivos seleccionados (bien sea la original o una ubicación personalizada en el equipo de destino):

%ARCHIVOS DE PROGRAMA% *o* ***C:\Archivos de programa***

%SYSTEM% *o* ***C:\Windows\System32****.*

La acción solicitada se envía a los equipos objetivo inmediatamente o tan pronto como vuelven a estar en línea. Una vez que un archivo se restaura, la entrada correspondiente desaparece de la la tabla de cuarentena

Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Este ajuste puede modificarse editando la política asignada a los equipos.

4.16 Registros

La consola de Bitdefender Cloud Security for Endpoints registra todas las operaciones y acciones ejecutadas por los usuarios. Los eventos registrados incluyen los siguientes:

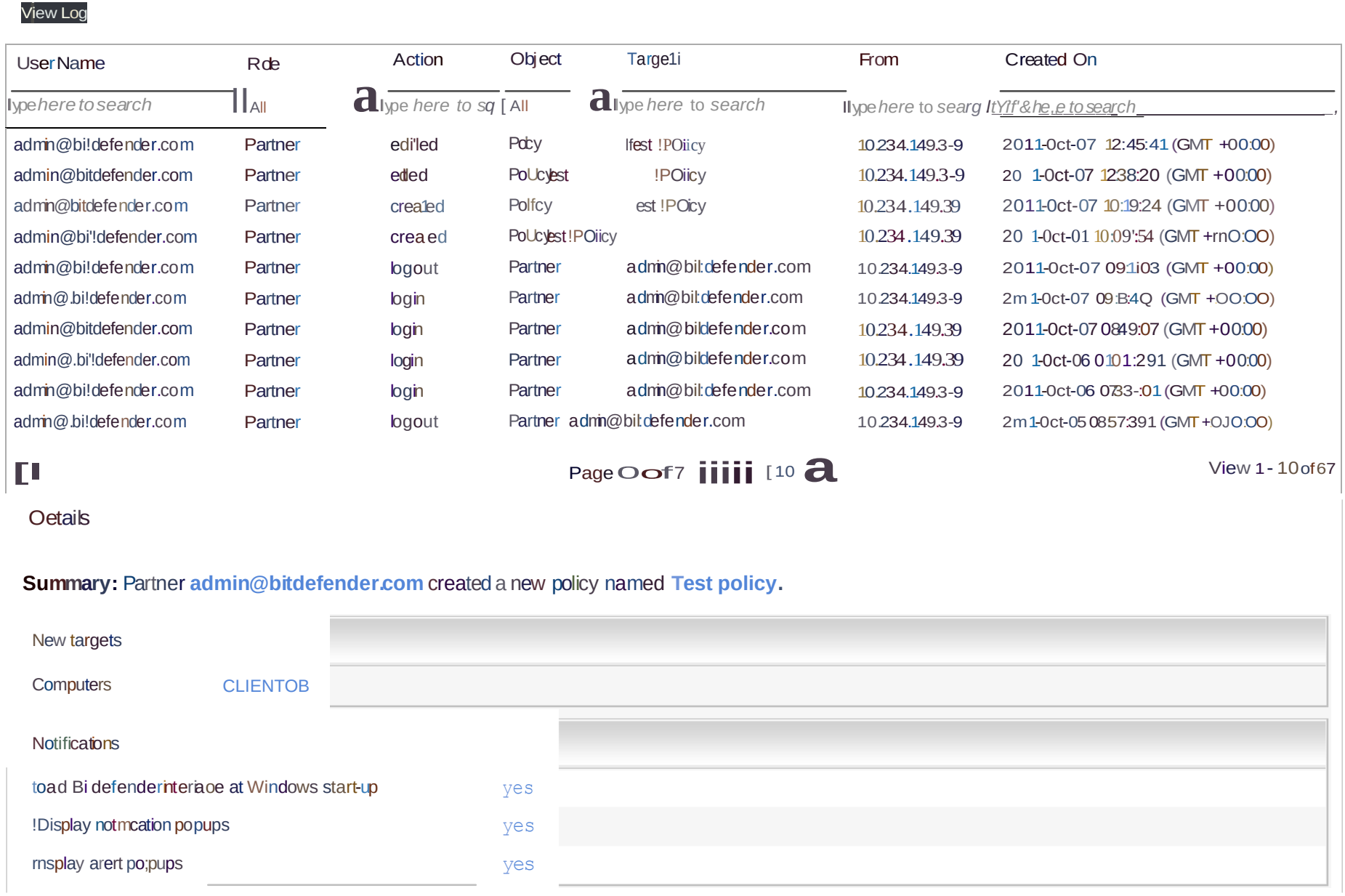
- Iniciar y cerrar sesión
- Crear, editar, renombrar, eliminar cuentas de usuario
- Crear, editar, renombrar, eliminar políticas
- Crear, editar, renombrar, eliminar informes
- Eliminar, restaurar archivos en cuarentena
- Eliminar o mover equipos entre grupos
- Crear, mover, renombrar, eliminar grupos

Haciendo clic en cada registro podrá mostrar los detalles del registro, tales como un breve resumen de las operaciones ejecutadas (usando variables), los equipos objetivo, etc.

Por ejemplo, en un registro de política encontrará los detalles de configuración de la política.

4.16 Registros

Bitdefender®



4.17 Licencias

- El proceso de licencia se basa en el punto final protegido (desktop o servidores)

- Modelos de suscripción **mensual** (nuevo) y de **1/2/3 años** (actual)

- La tarifa se basa en los **puntos finales** protegidos (incluyendo portátiles, desktops y servidores)

- Los partners gestionan el proceso de licencia – se encargan de proporcionar las licencias a los clientes

- Solamente se informará a los clientes sobre cuándo caducará el producto

- Los clientes no gestionarán las claves de licencia

- La cuenta inicial creada es la cuenta de evaluación de 30 días – el producto es completamente operativo

- Descuentos otorgados para educación, gobiernos, CUPG y renovación

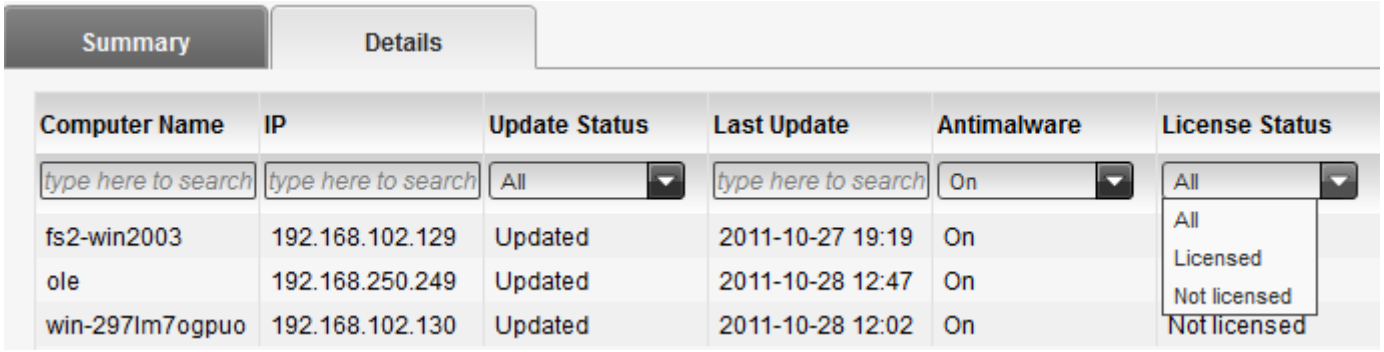
- La clave de licencia es una cadena con 7 caracteres alfanuméricos

4.17 Licencias

La información de licencia puede encontrarse en **la Security Console**:

Los equipos con licencia y sin licencia se presentan en las rutas indicadas a continuación:

- **Panel de control**, portlet del **Estado del equipo**

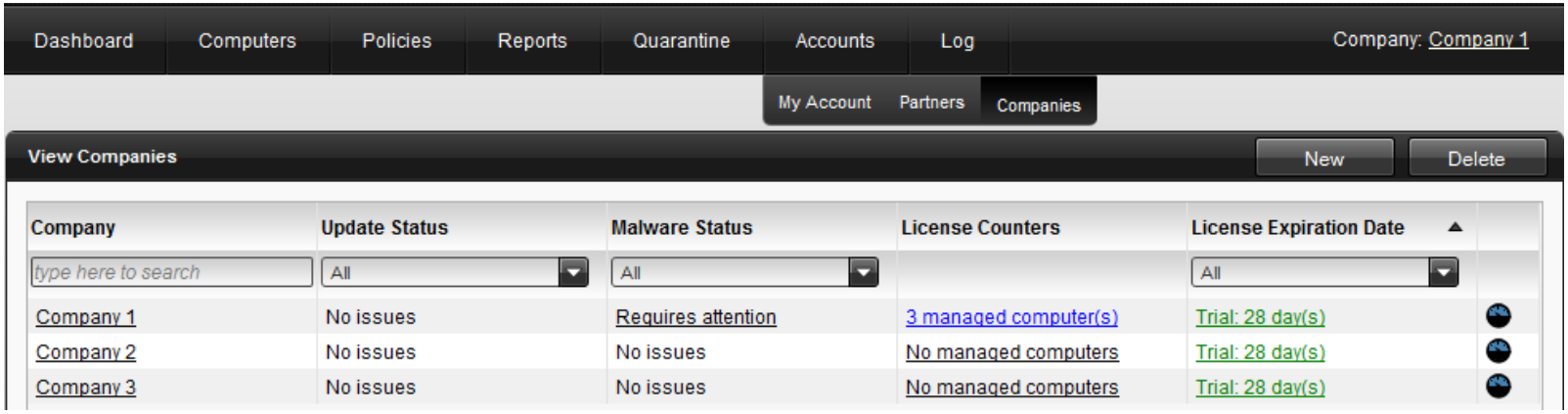


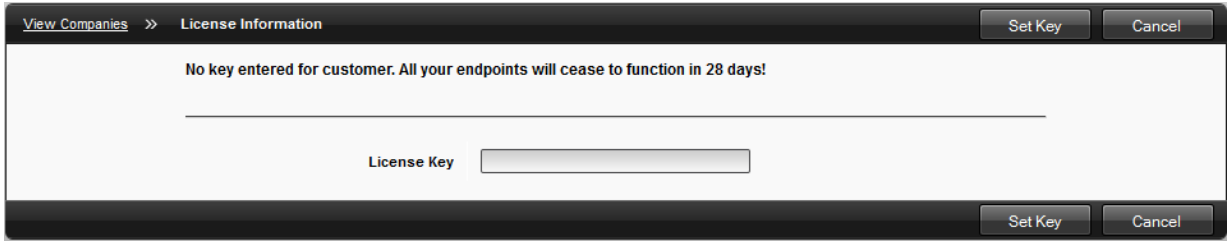
- **Equipos, Ver equipos, Informes, Estado del equipo**
- **Informes**, **Nuevo informe**, **Estado del equipo**
- **Equipos, Ver equipos,** haga clic en un equipo, detalles del equipo

4.17 Licencias

La información de Contadores de licencia y Caducidad de licencia también está disponible en la Security Console:

-**Cuentas**, **Empresas**



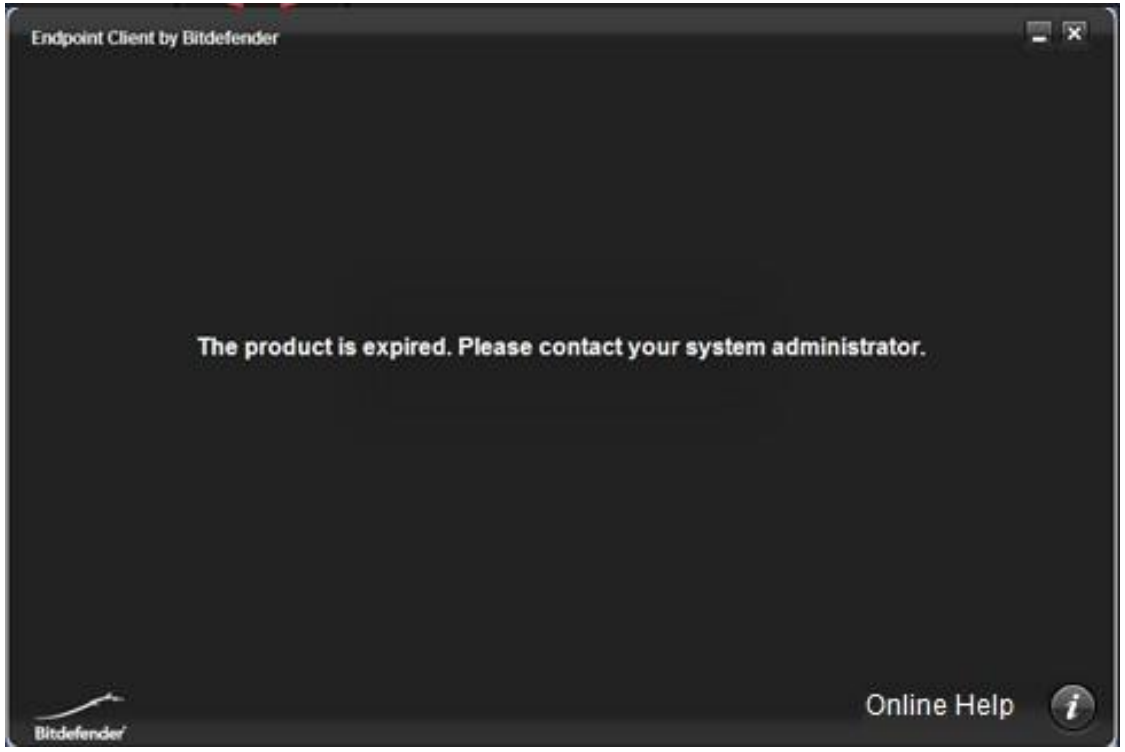


Los **contadores de licencia** indicarán cuántas claves de licencia están en uso del número total permitido para la clave correspondiente (por ejemplo 3 / 100). La **fecha de caducidad de la licencia** indicará el diferente estado que puede tener un cliente desde el punto de vista de la licencia (Evaluación = 30 días, Pendiente = desde el momento en el que se introduce la clave hasta que es autenticado, etc.)

4.17 Licencias

En el **Endpoint Client** – notificación de término de licencia

El producto ha caducado. Por favor, contacte con su administrador del sistema.



4.18 Resolución de problemas – Validar la instalación

CARPETAS DE INSTALACIÓN (máquina con Endpoint Client)

C:\Archivos de programa\Bitdefender\Endpoint Client by Bitdefender

C:\Archivos de programa\Common Files\Bitdefender

C:\ProgramData\Bitdefender

o

C:\Documents and Settings\All Users\Application Data – *para Windows XP*

4.18 Resolución de problemas – Validar la instalación

SERVICIOS que deberían enumerarse (máquina con Endpoint Client)

epcsrv.exe

Visualización del nombre: **Endpoint Client de Bitdefender**

Descripción: *ofrece protección contra malware y otras amenazas de la seguridad*

epupdsrv.exe

Nombre en pantalla: **Servicio de actualización de Endpoint Client de Bitdefender**

Descripción: *Descarga actualizaciones de Bitdefender y nuevas firmas malware desde Internet*

epag.exe

Nombre en pantalla: **Endpoint Agent de Bitdefender**

Descripción: *Asegura la comunicación entre una máquina cliente administrada y el servidor de seguridad*

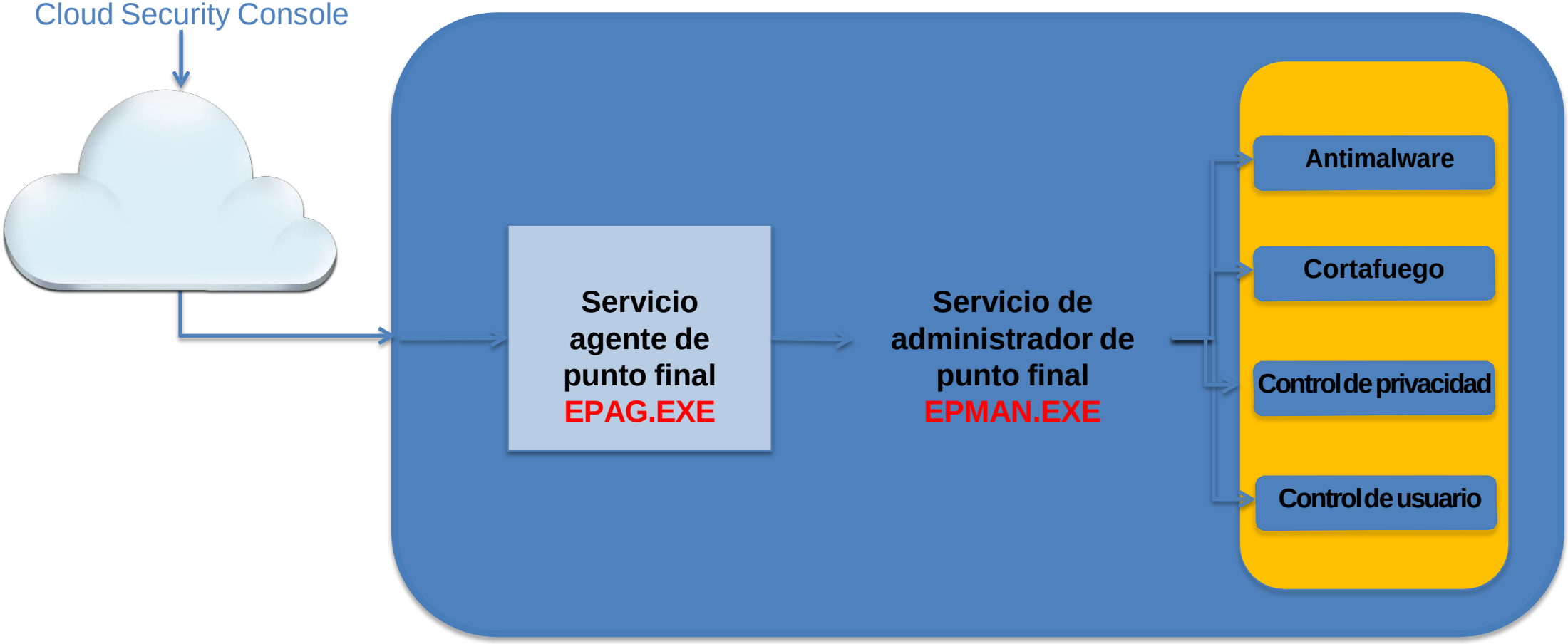
epman.exe

Visualización del nombre: **Endpoint Manager de Bitdefender**

Descripción: *Aplica la configuración del servidor de seguridad a un producto cliente administrado*

4.19 Detalles de los servicios de Endpoint Client

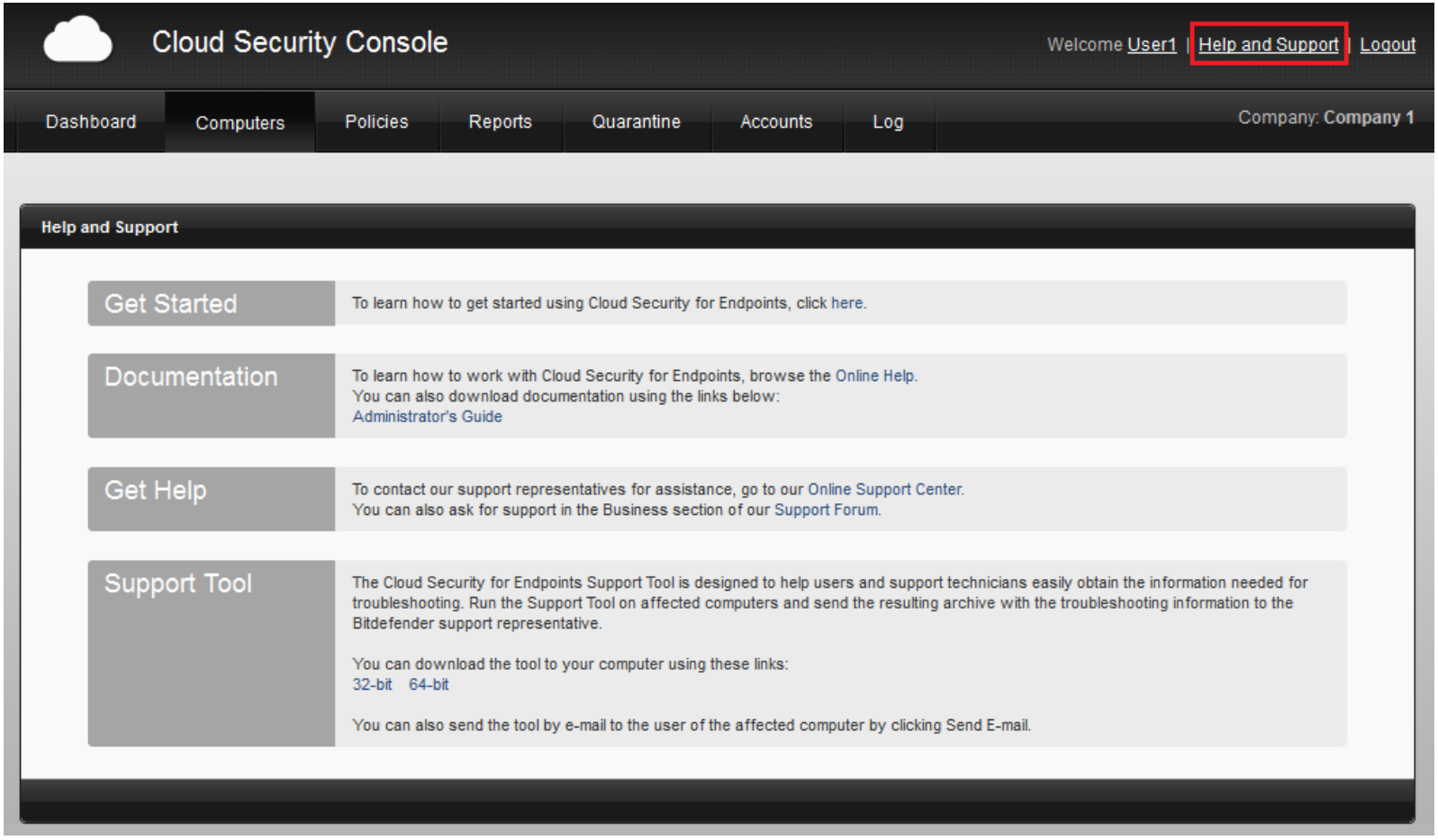
Cloud Security Console



4.20 Ayuda y soporte

Desde la interfaz principal de Cloud Security Console podrá acceder a la página de la sección **Ayuda y soporte**:

- Inicio
- Documentación
- Obtener Ayuda
- Herramienta de Soporte (para Win x86, x64)



5. Client Security vs. Cloud Security for Endpoints

	Client Security v3.5	Cloud Security for Endpoints
Descripción	Solución on-premise	- **No** es una solución on-premise - No reemplaza a Client Security 3.5 o una versión anterior - No requiere hardware en el emplazamiento
Servidor de administración y actualización	On premise	Cloud (mismo kit usado para estaciones de trabajo y servidores. Sin instalación de servidor de administración en el sitio)
Componentes	Management Server, BD Agent, Servidor de actualización, Consola, Business Client	Cloud Security Console y Endpoint Client
Administración Remota	Consola MMC	A través de la consola Web – Cloud Security Console (solo se necesita acceso a Internet)
Integración de Active Directory	Sí	No implementado todavía
Scripts WMI	Si	No implementado todavía
Informes de Auditoría	Sí	No
Cliente antispam	Sí	No
Crear Copia	Sí	No
Modo cliente	Usuario avanzado y usuario limitado	Configurado y administrado de forma remota por el administrador de red o el proveedor de servicios
Control del tráfico Web basado en categorías	No	Sí
Administración de políticas	1 plantilla de políticas / módulo de seguridad	1 plantilla de políticas para todos los módulos de seguridad

Bitdefender